MORECAMBE ROAD SCHOOL
GDPR Data Protection Policy

Statement of Intent

Morecambe Road School is required to keep and process certain information about its pupils staff, parents or carers and other individuals who come into contact with the school. This is in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR. All staff are involved with and have responsibility for the collection, processing and disclosure of personal data and must be aware of their duties and responsibilities by adhering to this policy and the law.

Organisational methods for keeping data secure are imperative, and Morecambe Road School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018. The government confirmed that the UK's decision to leave the EU does not affect compliance with GDPR.

The Data Protection Officer is the School Business Manager and can be contacted by the school telephone number 01524 414384 or email f.gill@morecamberoad.lancs.sch.uk

Appendix A – Data Protection Impact Assessment
Appendix B – Breach Report Form
Appendix C – Security and Breach Management Plan
Appendix D – Photos and Videos in School
Appendix E – Data Retention Schedule (IRMS Version 6)

Review

This policy will be reviewed regularly.

Policy approved by the Full Governing Body on 8th November 2023

Signed: ___Sarah Mainwaring_____ (Chair of Governors)

Signed: ___Anna Dootson_____ (Headteacher)

Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR) May 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to guidance from the Information Commissioner's Office.

Other School Policies Relating to GDPR Data Protection

Staff (including Volunteers and Agency Workers) should also refer to the following polices in relation to GDPR Data Protection:

- Child Protection and Safeguarding
- E Safety and ICT Security Policy
- Staff Code of Conduct including Agency Staff
- Non-Disclosure and Confidentiality Agreement
- Governors Code of Conduct
- Volunteer in School Policy
- Complaints Policy
- PSHE
- Freedom of Information Access
- National Curriculum
- School Admissions
- Staff Disciplinary and Grievance
- Special Educational Needs
- Whistleblowing by an Employee (Included the School Finance Manual)

Types of Data

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health and social matters.

1. Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

2. Accountability

Morecambe Road School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The school will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

3. Data Protection Officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.

- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

The DPO will report to the highest level of management at the school, which is the Headteacher.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

The DPO will work with the Governing Body to audit and report on DP

4. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed.

Under the GDPR, data will be lawfully processed under the following conditions:
- The consent of the data subject has been obtained.
- Processing is necessary for:
— Compliance with a legal obligation.
— The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
— For the performance of a contract with the data subject or to take steps to enter into a contract.
— Protecting the vital interests of a data subject or another person.

— For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:

— Carrying out obligations under employment, social security or social protection law, or a collective agreement.
— Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
— The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
— Reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards.
— The purposes of preventative or occupational medicine, for assessing the working capacity of the employee and medical diagnosis.
— Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
— Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

5. Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. The Primary contact on SIMS will be used for consent of pupil data.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn in writing by the individual at any time.

For all pupils at Morecambe Road School, up to and including Year 11, parental consent will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

6. The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge. The Privacy Notices for Parents and Pupils are published on the school website. The Parent Privacy Notice is issued to parents on admission of the pupil. Staff are issued with the Privacy Notice during induction with the School Business Manager.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:

— Withdraw consent at any time.
— Lodge a complaint with a supervisory authority.

- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

7. The right of access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The school will centrally record all SARs whether in writing or verbally. A SAR is different to Freedom of Information – please refer to FOI statement.

The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

8. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

9. The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest

- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed for the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- Legal compliance with completing a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific and/or historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

10. The right to restrict processing

Individuals have the right to block or suppress the school's processing of personal data.

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school will inform individuals when a restriction on processing has been lifted.

11. The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

The school will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to object

The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

13. Automated decision making and profiling

School does not engage with automated decision making and or profiling. This ensures that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of a decision and challenge it.

14. Privacy by design and privacy impact assessments

The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. The originator/person leading a new project for IT software/platform/application, or other system relating to data usage, is to complete the template DPIA – see Appendix A. On completion the assessment is to be emailed to the DPO for checking. New systems or procedures which include staff or pupil data must not be used until the DPIA is finalised by the DPO.

DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

Where a DPIA indicates high risk data processing, the DPO will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

15. Data breaches

The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their induction and CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach and action taken
- A description of the proposed measures to be taken to deal with the personal data breach

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

The breach report form can be found at Appendix B and the Security Breach Prevention and Management Plan at Appendix C. The form is to be completed by staff and handed immediately to the DPO who will then decide further steps eg refresher training. The DPO will enter the breach and subsequent action on the Breach Log for School.

16. Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff will not use their personal I Pads, pen drives, laptops or computers for school purposes.

Governors are to ensure that school documents are not retained with personal and identifiable data. Their home computers and laptops are to have passwords and checked for encryption.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by email, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data. Each class are provided with a Confidential Red Wallet which has a break clip to ensure non-tamper. Additional wallets and clips can be obtained from the DPO.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Morecambe Road School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

17. Publication of information

Morecambe Road School has a publication scheme outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Classes of information can be made available quickly and easily on request.

Morecambe Road School will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

18. CCTV and photography

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. Consent is requested and recorded for all members of staff, governors and pupils.

The school uses photographs of pupils to promote the learning within school and communicate to stakeholders. Staff will check permission and confirm prior to publishing photographs or videos.

Precautions, as outlined in Appendix C Photography and Videos at School, are taken when publishing photographs of pupils, in print, video or on the school website.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR. Parents are reminded to photograph or video their own child only and exclude all other children, unless they have agreement from other parents eg friendship groups.

The school does not collect CCTV images.

.

19. Data retention

Data will not be kept for longer than is necessary and in line with the IRMS Retention Schedule – see Appendix E

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Staff are to termly check their folders on the computer drives for unrequired and unlawful data, such as photos of ex pupils and staff.

20. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Copies of DBS certificates will not be retained within staff files.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Privacy Impact Assessments

Privacy impact assessments (PIAs) allow schools to consider the privacy issues relating to any personal information used within its projects.

A PIA will allow schools to identify and fix problems at an early stage.

A PIA should be completed by a member of staff who has responsibility for the processing of the project information.

The Information Commissioners Office provide guidance on:
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

PRIVACY IMPACT ASSESSMENT

Step one: About the project

What is the project name?	
What are the project objectives?	
Is there a project manager?	
Who are the customers?	
Who are the stakeholders?	
How long is the project due to last?	
What benefits will the project bring to the school, individuals and to other parties?	
What personal information is being used? Name, address, NI number, date of birth, gender, religion, occupation, medical history, ethnic origin, other?	
What is your legal basis for processing this information? • Consent • Legal Obligation • Contract • Vital Interests • Public Interest	

Step two: Describe the information flows

If you are using consent, how are you collecting the data subjects consent to process their personal information?	
What information are you collecting from the data subject?	
How will the information be collected?	
How will the information be used?	
Who will the information be shared with?	
If the information will be shared with suppliers, do we have a contract in place with the supplier?	
If the information will be shared with partners, do we have an information sharing agreement in place?	
Who will have access to the information?	
How long will the information be retained?	
How and when will the information deleted?	

Step three: Identify the privacy and related risks

Are there any risks to individual's privacy?	
Are there any risks to compliance with the law e.g. Data Protection Act, GDPR, PECR, Human Rights Act.	
Are there any risks to the school's reputation or finances?	
How will you check that the personal information used is accurate and complete?	
Have you set a retention period so that the information is not kept longer than necessary?	
Is the information being stored securely?	
Is the information being transferred to another country?	

Step four: Identify privacy solutions

Please list any risks and mitigating actions below.

Repeat the following for each risk.

Risk ID	Unique project risk id
Risk Description	[Event that has an effect on objectives] **caused by** [cause/s] **resulting in** [consequence/s]. 1. What could happen (event) 2. Why could it happen (caused by) 3. Resulting in (consequences)
Risk Type	• Political • Economic • Social • Technological • Legal • Environmental • Democratic • Organisational
Possible Consequences	What could happen if no action was taken to control the risk?
Current Situation	What is the current situation before any mitigating actions are taken?
Current Risk Score	Risk Score = likelihood x Impact.
Mitigating Actions	What mitigating actions are you taking to reduce the risk?
Residual Risk Score (after mitigating actions)	Risk Score = likelihood x Impact.
Risk Owner	Who owns the risk?
Direction of Travel	What is the direction of travel? Upwards or downwards or static.

How to score your risks

	CATASTROPHIC	5	10	**15**	**20**	**25**
	MAJOR	4	8	**12**	**16**	**20**
	MODERATE	3	6	9	**12**	**15**
IMPACT	MINOR	2	4	6	8	10
	INSIGNIFICANT	1	2	3	4	5
		RARE	UNLIKELY	POSSIBLE	LIKELY	CERTAIN
			LIKELIHOOD			

Step five: Sign off

Privacy risks and mitigating actions approved by|:

- Name:
- Signature:
- Date:

Step six: Integrate these risks and mitigating actions back into the project plan and review at each project meeting

November 2023

On completion, pass form to the DPO (School Business Manager) immediately

Report completed by : _____ Date: _____

Date of Breach:
Number of people affected:
Type of Breach:
Breach made by:
Description of breach:
How did the school become aware of the breach:
Who became aware of the breach:
Date on which the school became aware of the breach:
Consequences of the breach:
Action Taken:
Affected people informed:
Raised to the ICO and Date:
IF no, why not?:
If raised, by who:
Further training/action required:

Security Breach Prevention and Management Plan

Statement of intent

Morecambe Road School is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

The school recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing procedures to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

For the purposes of this policy, the title of '**data controller**' will be used in reference to the person(s) primarily responsible for the handling and protection of information and data within a school.

1. Types of security breach and causes

Unauthorised use without damage to data – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.

Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data.

Negligence, e.g. as a result of an employee that is aware of school policies and procedures, but disregards these.

Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the school software is more vulnerable to a virus

Incorrect firewall settings are applied, e.g. access to the school network, meaning individuals other than those required could access the system

Confusion between backup copies of data, meaning the most recent data could be overwritten

2. Roles and responsibilities

The Headteacher is responsible for implementing effective strategies for the management of risks posed by internet use, and to keep its network services, data and users secure.

The Data Protection Officer (SBM) is responsible for the overall monitoring and management of data security. Also responsible for establishing a procedure for managing and logging incidents.

The Governing Body is responsible for strategic compliance of data protection.

All members of staff and pupils are responsible for adhering to the processes outlined in this and the GDPR policy, alongside the school's E-Safety Policy and Acceptable Use Policy.

Secure configuration

An inventory/asset register will be kept of all IT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. This will be stored in the school systems and will be audited on an annual basis to ensure it is up-to-date.

Any changes to the IT hardware or software will be documented using the register.

IT support within school will audit regularly to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and is to be recorded.

Any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.

All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed on a termly basis to prevent access to facilities which could compromise network security.

The school believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

3. Network security

The school will employ firewalls in order to prevent unauthorised access to the systems. The school's firewall will be deployed as a **Centralised deployment**: the broadband service connects to a firewall that is located within a data centre or other major network location. Any compromise of security through the firewall will be reported to the DPO.

4. Malware prevention

The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

The IT co-ordinator will ensure that all school devices have secure malware protection and undergo regular malware scans. The IT co-ordinator will update malware protection on a regular basis to ensure it is up-to-date and can react to changing threats.

Malware protection will also be updated in the event of any attacks to the school's hardware and software.

Filtering of websites, as detailed in section 7 of this policy, will ensure that access to websites with known malware is blocked immediately and reported to the DPO (SBM).

Staff must be vigilant regarding malware that is transmitted by email. Caution is to be used with regard to spam or other messages which are designed to exploit users.

The IT co-ordinator will review the mail security technology on a regular basis to ensure it is kept up-to-date and effective.

5. User privileges

The school understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

The IT co-ordinator will ensure that user accounts are set up to allow users access to the facilities required, in line with the DPO and Headteacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

The IT co-ordinator will ensure that websites are filtered for inappropriate and malicious content. Any member of staff or pupil that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in section 12 of this policy.

All users will be required to change their passwords on a regular basis and must ensure that passwords are strong. Users will also be required to change their password if they become known to other individuals. Pupils are responsible for remembering their passwords; however, the IT co-ordinator will have an up-to-date record of all usernames and passwords, and will be able to reset them if necessary.

Pupils in KS1 will not have individual logins, and class logins will be used instead. If it is appropriate for a pupil to have an individual login, the IT co-ordinator will set up their individual user account, ensuring appropriate access and that their username and password is recorded.

Only individual accounts will be used for staff and older students.

The IT co-ordinator will manage this provision to ensure that all users are up to date and deleted when leaving school so that they do not have access to the system.

The IT co-ordinator will review the system on a regular basis to ensure the system is working at the required level.

6. Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

The school will inform all pupils and staff that their usage will be monitored, in accordance with the school's Acceptable Use Policy and E-Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the data controller. Alerts will also be sent for unauthorised and accidental usage.

Alerts will identify: the user, the activity that prompted the alert and the information or service the user was attempting to access.

All incidents will be responded to in accordance with this policy, and as outlined in the E-Safety Policy and Staff Disciplinary Policy.

7. Removable media controls and home working

The school understands that pupils and staff may need to access the school network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The IT co-ordinator will encrypt all school-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Pupils and staff are not permitted to use their personal devices where the school shall provide alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the Headteacher.

If pupils and staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the school's network security. This can be checked by the IT co-ordinator.

When using laptops, tablets and other portable devices, the Headteacher will determine the limitations for access to the network, as described in section 5 of this policy.

Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off school premises.

The IT co-ordinator will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises.

The school uses tracking technology where possible to ensure that lost or stolen school devices can be retrieved.

All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

The Wi-Fi network at the school will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise by the Headteacher.

8. Backing-up data

Back-ups are run overnight and are completed before the beginning of the next school day.

Upon completion of back-ups, data is stored externally by the schools IT third party support.

Only authorised personnel are able to access the school's data.

9. User training and awareness

The DPO will inform staff of network drives and passwords on their induction. New staff are to complete the online GDPR Training. All staff are to complete the DP online training annually in September.

Training for all staff members will be arranged by the Data Protection Officer within two weeks following an attack or significant update.

Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the E-Safety Policy.

10. Security breach incidents

Any individual that discovers a security data breach will report this immediately to the Data Protection Officer (SBM) using the Data Breach Report Form at Appendix B

The school's DPO will take the lead in investigating the breach, and will be allocated the appropriate time and resources to conduct this. The DPO, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or compromised. The DPO will oversee a full investigation and produce a comprehensive report. The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

If the DPO determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access.

The Headteacher will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-safety Policy.

The DPO will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes. Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups. Where the security risk is high, the school will establish what steps need to be taken to prevent further data loss which will require support from various school departments and staff.

This action will include:

Informing the ICO
Informing relevant staff of their roles and responsibilities in areas of the containment process.
Taking systems offline.
Retrieving any lost, stolen or otherwise unaccounted for data.
Restricting access to systems entirely or to a small group.
Backing up all existing data and storing it in a safe location.
Reviewing basic security, including:
Changing passwords and login details on electronic equipment.
Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach. The DPO will arrange for testing of all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the school's systems are safe to use.

11. Assessment of risks

The following questions will be considered by the DPO in order to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the data controller's report and records:

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the GDPR 2018; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
- Has individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?
- Could harm come to individuals? This could include risks to the following:
- Physical safety
- Emotional wellbeing
- Reputation
- Finances
- Identity
- Private affairs becoming public

- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the school's reputation, or risk to the school's operations?
- Who could help or advise the school on the breach? Could the LA, external partners, authorities, or others provide effective support?

In the event that the DPO, or other persons involved in assessing the risks to the school, are not confident in the risk assessment, they will seek advice from the Information Commissioner's Office (ICO).

12. Consideration of further notification

The school will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security.

The school will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

If a large number of people are affected, or there are very serious consequences, the ICO will be informed.

The school will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included.
- Specific and clear advice on the steps they can take to protect themselves, and what the school is willing to do to help them.
- A way in which they can contact the school for further information or to ask questions about what has occurred.

The school will consult the ICO for guidance on when and how to notify them about breaches. The school will consider, as necessary, the need to notify any third parties – police, insurers, professional bodies, funders, trade unions, website/system owners, banks/credit card companies – who can assist in helping or mitigating the impact on individuals.

Under the GDPR, the following steps will be taken if a breach of personal data occurs:

The school will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in significant risk to the rights and freedoms of individuals, the school will notify those concerned directly with the breach.

Where the breach compromises personal information, the notification will contain:

- The nature of the personal data breach including, where possible:
- The type(s), e.g. staff, pupils or governors, and approximate number of individuals concerned.
- The type(s) and approximate number of personal data records concerned.
- The name and contact details of the DPO or other person(s) responsible for handling the school's information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

13. Evaluation and response

The DPO will establish the root of the breach, and where any present or future risks lie.

The DPO will consider the data and contexts involved.

The DPO and Headteacher will identify any weak points in existing security measures and procedures.

The DPO and Headteacher will identify any weak points in levels of security awareness and training.

The DPO will report on findings and, with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

Timeline of Incident Management

Date	Time	Activity	Decision	Name/position	Date

APPENDIX D

Photography and Videos at School

Statement of intent

At **Morecambe Road School**, we use imagery and videos for a variety of purposes, including prospectuses, display boards, educational purposes, conferences and the school website. We understand that parents may also wish to take videos or photos of their children participating in school events for personal use.

Whilst we recognise the benefits of photography and videos to our school community, we also understand that these can have significant risks for those involved. Under the legal obligations of the General Data Protection Regulation (GDPR), the school has specific responsibilities in terms of how photos and videos are taken, stored and retained.

The school has implemented a policy on the safe use of cameras and videos by staff and parents to reflect the protective ethos of the school with regard to pupils' safety.

In order to ensure that, as far as possible, the use of photography and video is used safely at all times, the policy provided below should be followed. This policy is applicable to all forms of visual media, including film, print, video, DVD and websites.

Definitions

For the purpose of this policy:

"Personal use" of photography and videos is defined as the use of cameras to take images and recordings of children by relatives, friends or known individuals, e.g. a parent taking a group photo of their child and their friends at a school event. These photos and videos are only for personal use by the individual taking the photo, and are not intended to be passed on to unknown sources. The principles of the GDPR do not apply to images and videos taken for personal use.

"Official school use" is defined as photography and videos which are used for school purposes, e.g. for building passes. These images are likely to be stored electronically alongside other personal data. The principles of the GDPR apply to images and videos taken for official school use.

"Media use" is defined as photography and videos which are intended for a wide audience, e.g. photographs of children taken for a local newspaper. The principles of the GDPR apply to images and videos taken for media use.

Staff may also take photos and videos of pupils for **"educational purposes**". These are not intended for official school use, but may be used for a variety of reasons, such as school displays, special events, assessment and workbooks. The principles of the GDPR apply to images and videos taken for educational purposes.

1. Roles and responsibilities

The Headteacher is responsible for:

- Liaising with social workers to gain consent for photography and videos of LAC pupils.
- Liaising with the data protection officer (DPO), to ensure there are no data protection breaches.
- Informing relevant bodies of any known changes to a pupil's security, e.g. child protection concerns, which would mean that participating in photography and video recordings would put them at significant risk.
- Submitting consent forms to parents with regards to photographs and videos being taken whilst at school.
- Ensuring that all photos and videos are stored and disposed of correctly, in line with the GDPR.
- Deciding whether parents are permitted to take photographs and videos during school events.
- Communicating this policy to all the relevant staff members and the wider school community, such as parents.

Parents are responsible for:

- Completing the Consent Form.
- Informing the school in writing where there are any changes to their consent.
- Acting in accordance with this policy.

In accordance with the school's requirements to have a DPO, the DPO is responsible for:

- Informing and advising the school and its employees about their obligations to comply with the GDPR in relation to photographs and videos at school.
- Monitoring the school's compliance with the GDPR in regards to processing photographs and videos.
- Advising on data protection impact assessments in relation to photographs and videos at school
- Conducting internal audits, in regards to the school's procedures for obtaining, processing and using photographs and videos.
- Providing the required training to staff members, in relation to how the GDPR impacts photographs and videos at school.

2. Parental consent

The school understands that consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given and last updated.

The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease.

Where a child is under the age of 16, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

All parents will be asked to complete the Consent Form, which will determine whether or not they allow their child to participate in photographs and videos.

Consent will be valid unless changed in writing by the parent. With respect to media photographs, such as printed marketing material and the school website, this may extend past the child leaving Morecambe Road School.

If there is a disagreement over consent, or if a parent does not respond to a consent request, it will be treated as if consent has not been given, and photographs and videos will not be taken or published of the pupil whose parents have not consented.

All parents are entitled to withdraw or change their consent at any time during the school year but must do so in writing.

For any LAC pupils, or pupils who are adopted, the DSL will liaise with the pupil's social worker, carers or adoptive parents to establish where consent should be sought. Consideration will be given as to whether identification of an LAC pupil, or pupils who are adopted, would risk their security in any way.

Consideration will also be given to any pupils for whom child protection concerns have been raised. Should the DSL believe that taking photographs and videos of any pupils would put their security at further risk, greater care will be taken towards protecting their identity.

A list of all the names of pupils for whom consent was not given will be created by the School Office and will be circulated to all staff members. This list will be updated as and when there are changes. Staff can also check pupil consent via SIMS

If any parent withdraws or changes their consent, or the DSL reports any changes to a pupil's security risk, or there are any other changes to consent, the list will also be updated and re-circulated.

3. General procedures

Photographs and videos of pupils will be carefully planned before any activity.

Where photographs and videos will involve LAC pupils, adopted pupils, or pupils for whom there are security concerns, the Headteacher will determine the steps involved.

When organising photography and videos of pupils, the Headteacher, as well as any other staff members involved, will consider the following:

Can general shots of classrooms or group activities, rather than individual shots of pupils, be used to fulfil the same purpose?

Could the camera angle be amended in any way to avoid pupils being identified?

Will pupils be suitably dressed to be photographed and videoed?

Will pupils of different ethnic backgrounds and abilities be included within the photographs or videos to support diversity?

Would it be appropriate to edit the photos or videos in any way? E.g. to remove logos which may identify pupils?

Are the photographs and videos of the pupils completely necessary, or could alternative methods be used for the same purpose? E.g. could an article be illustrated by pupils' work rather than images or videos of the pupils themselves?

The list of all pupils of whom photographs and videos must not be taken will be checked prior to the activity. Only pupils for whom consent has been given will be able to participate.

The staff members involved will liaise with the Deputy Headteacher if any LAC pupil, adopted pupil, or a pupil for whom there are security concerns is involved.

School equipment will be used to take photographs and videos of pupils.

Staff will ensure that all pupils are suitably dressed before taking any photographs or videos.

Where possible, staff will avoid identifying pupils. If names are required, only first names will be used.

The school will not use images or footage of any pupil who is subject to a court order.

Photos and videos that may cause any distress, upset or embarrassment will not be used.

Any concern relating to inappropriate or intrusive photography or publication of content is to be reported to the DPO.

4. Additional safeguarding procedures

The school understands that certain circumstances may put a pupil's security at greater risk and, thus, may mean extra precautions are required to protect their identity.

The DSL will, in known cases of a pupil who is an LAC or who has been adopted, liaise with the pupil's social worker, carers or adoptive parents to assess the needs and risks associated with the pupil.

Any measures required will be determined between the DSL, social worker, carers, DPO and adoptive parents with a view to minimise any impact on the pupil's day-to-day life. The measures implemented will be one of the following:

- Photos and videos can be taken as per usual school procedures
- Photos and videos can be taken within school for educational purposes and official school use, e.g. on registers, but cannot be published online or in external media
- No photos or videos can be taken at any time, for any purposes

Any outcomes will be communicated to all staff members via a staff meeting and the list outlining which pupils are not to be involved in any videos or photographs, held in the school office, will be updated accordingly. This is also recorded on pupil records on SIMS

5. School-owned devices

Staff are encouraged to take photos and videos of pupils using school IT equipment eg school Ipads; however, they may use other equipment, such as school-owned mobile devices, where the DPO has been consulted and consent has been sought from the Headteacher prior to the activity.

Where school-owned devices are used, images and videos will be provided to the school at the earliest opportunity, and removed from any other devices.

Staff will not use their personal mobile phones, or any other personal device, to take images and videos of pupils.

Photographs and videos taken by staff members on school visits may be used for educational purposes, e.g. on displays or to illustrate the work of the school, where consent has been obtained.

Digital photographs and videos held on the school's drive are accessible to staff only. Photographs and videos are stored in labelled files, annotated with the date, and are only identifiable by year group/class number – no names are associated with images and videos.

Folders on network drives containing photographs and videos are to be deleted as soon as the class/child leaves the school. This is the responsibility of class teams and a record is to be made on the T Drive – GDPR folder – Disposal of Data Log.

6. Use of a professional photographer

If the school decides to use a professional photographer for official school photos and school events, the Headteacher will:

Provide a clear brief for the photographer about what is considered appropriate, in terms of both content and behaviour.

Issue the photographer with identification, which must be worn at all times.

Let pupils and parents know that a photographer will be in attendance at an event and ensure they have previously provided consent to both the taking and publication of videos or photographs.

Not allow unsupervised access to pupils or one-to-one photo sessions at events.

Communicate to the photographer that the material may only be used for the school's own purposes and that permission has not been given to use the photographs for any other purpose.

Ensure that the photographer will comply with the requirements set out in GDPR.

Ensure that if another individual, such as a parent or governor, is nominated to be the photographer, they are clear that the images or videos are not used for any other anything other than the purpose indicated by the school.

7. Permissible photography and videos during school events

If the Headteacher permits parents to take photographs or videos during a school event, parents will:

Remain seated while taking photographs or videos during concerts, performances and other events.

Minimise the use of flash photography during performances.

In the case of all school events, make the focus of any photographs or videos their own children.

Avoid disturbing others in the audience or distracting pupils when taking photographs or recording video.

Ensure that any images and recordings taken at school events are exclusively for personal use and are not uploaded to the internet, posted on social networking sites or openly shared in other ways.

Refrain from taking further photographs and/or videos if and when requested to do so by staff.

8. Storage and retention

Images obtained by the school will not be kept for longer than necessary.

Hard copies of photos and video recordings held by the school will be annotated with the date on which they were taken and will be stored securely. They will not be used other than for their original purpose, unless permission is sought from the Headteacher and parents of the pupils involved and the DPO has been consulted.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Parents must inform the school in writing where they wish to withdraw or change their consent. If they do so, school will attempt to remove any related imagery and videos involving their children.

When a parent withdraws consent, it will not affect the use of any images or videos for which consent had already been obtained. Withdrawal of consent will only affect further processing.

Where a pupil's security risk has changed, if required, any related imagery and videos involving the pupil will be removed from the school drive immediately. Hard copies will be removed by returning to their parents or by shredding, as appropriate.

Official school photos are held on SIMS alongside other personal information, and are retained for the length of the pupil's attendance at the school, or longer, if necessary, e.g. due to a police investigation.

Some educational records relating to former pupils of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Toolkit for Schools

2019

irms

the interactive hub of the information world

From the Chair - IRMS
Scott Sammons

Dear Reader,

It is my pleasure to welcome you to this revised Information and Records Management Toolkit for Schools Version 6.0.

This toolkit has been made free of charge to non-members, however, if you would like a word version, you can sign up to IRMS for less than a £100 a year at **www.irms.org.uk/join.** Signing up as a member also entitles you to ask the author questions plus a lot of other benefits. So why not join your colleagues in the information field today and help us fund more useful toolkits like this one?!

I am a little biased (as an Information Geek and as Chair of the IRMS), but I firmly believe in the importance and value of good information and records management practices and this publication looks to assist in this important sector for a number of years to come. I am proud that the Information and Records Management Society (IRMS) has been able to review and maintain the accuracy of this document from the help of our volunteers.

If you're about to embark on reading through this toolkit and getting information handling right for your organisation I wish you all the very best and ensure you that you are in trusted hands. This toolkit is the combination of the knowledge, experience and brain wizardry of the IRMS and Kent County Council's Elizabeth Barber.

My thanks go to the Department for Education for their support of the free PDF toolkit that enables such greater access to records management advice on such an important topic especially with GDPR making schools realise they need this information.

My thanks also go to some key people that have been involved in the development of the toolkit, firstly, is Elizabeth Barber who has helped shape and drive the toolkit forward with such limited resource and we are forever in her debt.

Second is Keith Batchelor, he is known to many in the profession, has offered his experience, expertise and time free of charge to review the content for this toolkit.

My thanks also go to the wider content team for their time and input into ensuring the amazing content is up to date, the reviews and the critiques to getting the toolkit where it is today.

As a result, I look forward to hearing your stories of your information and records management journeys, both personally and for your organisations. May this toolkit be as useful to you as it has been to many others.

All the very best,

Scott

Scott Sammons FIIM, AMIRMS, Cert.NLP

Chair, IRMS 2019

978-1-9161239-1-5

From the Sponsor - Groupcall
Andrew Mulholland

It is our great pleasure to welcome you to the latest edition of the IRMS Records Management Toolkit for Schools. As a leader in data protection services for schools, trusts and local authorities, we are delighted to be sponsoring such a fantastic resource. Good records and information management is part and parcel of running a successful school - from the legal obligations around collection and retention right through to having solid, robust processes in place to keep that data safe whilst ensuring it is still accessible and manageable for the staff who need it.

Groupcall has a strong interest in helping schools develop robust data protection systems and processes. As well as having trained thousands of school leaders in data protection best practice, we also recently conducted a national survey to better understand how those practices have been embedded. This research highlighted that there are still gaps in data protection processes in many schools, with the most concerning being the number who still haven't appointed an appropriate data protection officer, with many school DPOs having conflicts of interest from their other roles in school. The research also revealed that many still struggle with data protection impact assessments and properly understanding the use of consent under the GDPR and DPA 2018.

The education industry also continues to be a major source of data breaches - often due to simple carelessness. Data protection is everybody's responsibility and having good records management structures in place for people to work with is key.

The situation is starting to become real from an enforcement standpoint, with the ICO already conducting audits in multi-academy trusts – and while large fines are unlikely to be imposed on educational organisations, the threat of reputational damage from mislaid data is real.

That's not to say it's all bad news. While there are concerns in a number of areas, we find schools are generally good at records management, especially when it comes to safeguarding and other statutory requirements. Schools also generally have good physical security in place, which is an important part of keeping information safe.

But – things can always be improved! And the fact that you've taken the time to download and digest this toolkit shows you are on the right track to better data management.

The IRMS is a fantastic organisation and we are thrilled to be able to help them make this best practice information available. We trust you will find it useful and wish you all the best in your continuing records management journey.

Andrew Mulholland
Director of Marketing
Groupcall

Contents

978-1-9161239-1-5

Contents

978-1-9161239-1-5

Introduction

The Information Management Toolkit for Schools has been created to assist schools with managing their information in line with the current legislative frameworks.

Module 1 consists of the base toolkit designed to assist schools, which are under local authority control, in their compliance with the Freedom of Information Act 2000.

Module 2 (currently under development) will consist of additional information which is designed to assist Academies in their compliance with the Freedom of Information Act 2000 and other business requirements.

Module 3 (currently under development) will consist of additional information which is designed to assist independent schools with managing their records in line with legislative requirements.

The Information Management Toolkit for Schools is being made available to schools free of charge in PDF format. The Toolkit is available in MSWord format at no additional charge to IRMS members and at a fixed charge to non-members. For more details about this please contact IRMS (info@irms.org.uk).

All questions, suggestions and amendments to the toolkit should be sent to schooltoolkit.irms.org.uk. We will only undertake to answer questions from IRMS members, so please include your IRMS membership number when sending the question.

The Information Management Toolkit for Schools is designed as guidance and should not be quoted to users as being a "standard". All local authorities should seek the advice of their own legal departments before using the toolkit. Local authorities should not refer members of the public to the IRMS for clarification about the toolkit. The IRMS is not a public body and therefore is not subject to the Freedom of Information Act 2000. All requests for information relating to the toolkit used by individual authorities must be addressed by that authority.

The review group consisted of the following members:

General Editor:

Elizabeth Barber	Kent County Council

Contributors:

Keith Batchelor	**Batchelor Associates – Records Management Consultants**
Andrea Binding	Somerset County Council
Andy Crow	Chorus Advisers
Lizi Bird	Solihull Metropolitan Borough Council
Sinead Booth	Data Protection
Ciara Carroll	Cirrus Primary Academy Trust
Natalie Fear	One West, Bath and North East Somerset Council
Catrina Finch	City of Wolverhampton Council
Claire Jurczuk	Department for Education
Molly Kirkham	Gloucestershire County Council
Thomas Ng	West Berkshire Council
Romin Partnovia	
Tony Sheppard	GDPR in Schools
Rebecca Taylor	Acorn Trust
Suzy Taylor	New College Durham
Alison Tennant	Liverpool Diocesan Trust
Joel Thornton	The Little IT Company

Proof Readers:

Dr Christopher Webb	Lambeth Palace
Nicola Kirwan-Williams	

Note from the Editor

The Information Management Toolkit for Schools contains a number of different fact sheets which have been compiled by various working groups within the Review Group. This means that there is not a consistency of language or presentation across the toolkit. For example, one working group may have written in the third person where another may not. It has been decided to retain the original format of the documents as they were supplied to the editor to reflect the diversity of the working groups.

Users of the toolkit should be aware that this toolkit was compiled for use by local authority schools. The IRMS is aware that local authority schools are fast becoming a thing of the past and the intention is to amalgamate this toolkit with the toolkit for Academies at the next review to reflect this.

Users of the toolkit should also be aware that this guidance was compiled whilst the Independent Inquiry Into Child Sexual Abuse (IICSA) was still sitting. At the time of writing there is a moratorium on the disposal of any material which may be required by the Inquiry, and instructions have been issued to organisations explaining what they need to do. If a school is unsure about how IICSA impacts a particular group of documents then they should seek advice from their local authority or legal advisers.

The Information Management Toolkit for Schools contains the following sections, which are hyperlinked from the contents page for ease of reference:

Records Management Policy
Each public authority (including individual schools) should have a records management policy. The Toolkit contains a Policy Document which can be adopted in its entirety or adapted to reflect the different needs of individual schools.

Pupil Records
Guidelines about what should be included in the main pupil record, plusadvice about what information should be transferred on to the next school as well as how this information should be transferred.

Records Management Programme
The Information Management Toolkit aims to assist individual schools with managing records throughout their lifecycle. There is advice about managing e-mail so as to ensure that it becomes part of the core record. There is also advice about how to conduct an information audit, along with some templates.

The 2018 revision of this toolkit contains three completely new sections. There is a section on managing compliance with GDPR for schools based on frequently asked questions, along with some templates. There is a section relating to the monitoring of electronic communication and the management of Social Media. The section on Information Security, Business Continuity and Digital Continuity has been completely remastered as part of this review.

There are also guidelines about what needs to be considered when a school closes or changes status. There is a checklist covering requirements for physical storage areas.

978-1-9161239-1-5

Records Management Policy

Background

Section 46 of the Freedom of Information Act 2000 requires schools, as public authorities, to follow a Code of Practice on managing their records. Under section 7 of the Code of Practice on the Management of Records, it states that:

"Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy."

This policy needs to:

1. Be endorsed by senior management, for example at board level, and should be readily available to staff at all levels. (section 7.1)
2. Provide a mandate for the records and information management function, and a framework for supporting standards, procedures and guidelines. The precise contents will depend on the particular needs and culture of the authority, but it should as a minimum:
   a. Set out the authority's commitment to create, keep and manage records which document its principal activities;
   b. Outline the role of records management and its relationship to the authority's overall business strategy;
   c. Identify and make appropriate connections to related policies, such as those dealing with e-mail, information security and data protection;
   d. Define roles and responsibilities, including the responsibility of individuals to document their work in the authority's records to the extent that, and in the way that, the authority has decided their work should be documented, and to use those records appropriately;
   e. Indicate how compliance with the policy and the supporting standards, procedures and guidelines will be monitored. (7.2)
3. The policy should be kept up-to-date so that it reflects the current needs of the authority, particularly given the rapidly changing technological environment and the embedding of the new data protection legislation. One way of ensuring this is to review it at agreed intervals, for example: annually; following an event which may require a review of practice (e.g. a subject access request); or after major organisational or technological changes, in order to assess whether it needs amendment. (7.3)
4. The authority should consider publishing the policy so that members of the public can see the basis on which it manages its records. (7.4)

[For a full copy of the Lord Chancellor's Code of Practice see http://www.nationalarchives.gov.uk/documents/information-management/foi-section-46-code-of-practice.pdf]

Having a records management policy will support the school in meeting its responsibilities under the Data Protection Act 2018 and the General Data Protection Regulation.

Policy Template

The following extract forms part of a policy statement template which could be adopted by individual schools. It has been extracted from a model action plan for developing records management compliant with the Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act 2000 Model Action Plan for Schools. https://www.nationalarchives.gov.uk/documents/schools.rtf

The policy statement template can be adopted in its entirety or can be amended to reflect the needs of individual schools. Once it has been amended, it should be approved by the governing body or other appropriate authority. Once the records management policy has been approved at the appropriate level it should be published, perhaps as part of the publication scheme.

[Name of School] Records Management Policy

The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability.

Records Management Policy Continued

This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies.

1. Scope of the policy

1.1 This policy applies to all records created, received or maintained by permanent and temporary staff of the school in the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the school.

1.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronic format e.g. paper documents, scanned documents, e-mails which document business activities and decisions, audio and video recordings, text messages, notes of telephone and Skype conversations, spreadsheets, Word documents, presentations etc.

2. Responsibilities

2.1 The governing body of a school has a statutory responsibility to maintain the school records and record keeping systems in accordance with the regulatory environment specific to the school. The responsibility is usually delegated to the headteacher of the school.

2.2 The person responsible for day-to-day operational management in the school will give guidance on good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.3 The school will manage and document its records disposal process in line with the Records Retention Schedule. This will help to ensure that it can meet Freedom of Information requests and respond to requests to access personal data under data protection legislation (subject access requests "SARS").

2.4 Individual staff and employees must ensure, with respect to records for which they are responsible, that they:

2.4.1 Manage the school's records consistently in accordance with the school's policies and procedures;

2.4.2 Properly document their actions and decisions;

2.4.3 Hold personal information securely;

2.4.4 Only share personal information appropriately and do not disclose it to any unauthorised third party;

2.4.5 Dispose of records securely in accordance with the school's Records Retention Schedule.

3. Relationship with existing policies

This policy has been drawn up within the context of:

- Freedom of Information policy
- Data Protection policy
- Information Governance Policy and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

Signed: [Head of School]

978-1-9161239-1-5

Creation and Management of School Archives

The National Archives has supplied the following information in relation to the creation and management of school archives:

If your school is keeping an archive (e.g. of old photographs/ registers), either at your local Record Office or at your school, it would be right to include a statement in your school's Data Protection Policy to advise the public that such archive is in place. This will help separate the personal data your school keeps for operational reasons and those for archive reasons and in turn a much more manageable way to deal with data subject requests. The following paragraph could be included:

The XXX school archive is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of school-life among many generations of Old XXXians; and to serve as a research resource for all interested in the history of XXX school and the community it serves.

Acknowledgements

Content developed in 2012 by:

Anthony Sawyer	Herefordshire Public Services
John Davies	TFPL Consultancy

Reviewed in 2018 by:

Thomas Ng	West Berkshire Council
Molly Kirkham	Gloucestershire County Council
Catrina Finch	City of Wolverhampton Council

Pupil Records: Guidance

Introduction

All schools, with the exception of independent schools, are under a duty to maintain a pupil record for each pupil. Early Years settings will have their own record keeping requirements.

The 'Pupil Record' comprising the educational and curricula record, should be seen as the core record charting the individual pupil's progress through the education system, and should accompany them throughout their school career. This record will serve as the formal record of their academic achievements, other skills and abilities, and progress in school.

The aim of this guidance is to provide some consistency of practice in the way in which pupil records are managed across all schools. It includes suggestions on the content of the pupil record, advice on transferring to the next school, and retention and disposal arrangements for both paper and electronic records.

Pupil Record

Recording and disclosure of information

Pupil records may be held in paper form, or else electronically (for instance as part of the school management information system (MIS)). Schools will have their own systems for maintaining pupil records, which may be a combination of electronic and hard copy files.

All information must be easy to find, accurately and objectively recorded and expressed in a professional manner as pupils and parents have a right of access to their educational record via two possible routes:

1. A request for an educational record.
   The Education (Pupil Information) (England) Regulations 2005, states that the pupil record must be provided to parents within 15 school days of a request where the pupil is enrolled in a maintained school. This provision does not apply to Academies, independent schools etc;
2. Requests for information by pupils, or their parents are to be treated as subject access requests under Data Protection legislation.

Paper Files

The following information is useful on the front of a paper file, if one is held:

- Surname and forename
- Date of birth
- Unique Pupil Number
- Date file was started/opened

It may be useful to have the following information inside the front cover so that it is easily accessible to authorised staff; this is not necessary if accessible on the school information management system:

- Emergency contact details
- Preferred name
- Names and contact details of adults who have parental responsibility/care for the pupil
- Reference to further information held on allergies/ medical conditions
- Other agency involvement e.g. SEN, speech and language therapist, etc.
- Reference to any other linked files

978-1-9161239-1-5

Contents of the pupil record

The table below lists common and potential record types that may form part of the Pupil Record.

Record Type	Notes
Record of transfer from Early Years setting	If applicable
Admission Form	
Data Collection/Checking Form – current	This should be checked regularly by parents to ensure details are accurate
Annual written report to parents	
National Curriculum and Religious Education locally agreed syllabus record sheets	
Any information relating to a major incident involving the child	
Statements/Plans, reports, etc. for educational support, e.g. SEN, Speech and Language	Store in a separate area of the record or keep in a separate linked file
Medical information relevant to the child's on-going education/behaviour	Store in a separate area of the record or keep in a separate linked file
Child protection reports/disclosures and supporting documentation	Store in a separate area of the record or keep in a separate linked file so as to limit access to specific staff
Any information relating to exclusions (fixed or permanent)	
Specific correspondence with parents or outside agencies relating to major issues	This may be in e-mail form. Once matter is closed save any correspondence that records sequence of events, pertinent issues and outcomes to pupil record
Summary details of complaints made by the parents or the pupil relevant to the child's on-going education/behaviour	This may be in e-mail form, see note above. Most complaints records are retained by the school and not as part of the pupil record
Examination Results – pupil copy	Send uncollected certificates back to exam board after all reasonable efforts to contact the pupil have been exhausted
SATS Results	A note of the result should be recorded

Pupil Records: Guidance Continued

Records not forming part of the pupil record

The following record types should be stored separately to the main pupil record, as they are usually subject to shorter retention periods (please see the Retention Schedule section); they should not be forwarded to the pupil's next school:

- Attendance Registers and Information
- Absence (authorised) notes and correspondence
- Parental consent forms for trips/outings
- Accident forms (a copy can be placed on the pupil record if it is a major incident)
- Medicine consent and administering records (this is the school's record)
- Copies of birth certificates, passports, etc.
- Generic correspondence with parents about minor issues (i.e. 'Dear Parent')
- Pupil work, drawings, etc.
- Previous data collection forms which have been superseded (there is no need to retain these)
- Photography (image) consents (this is the school's record).

Information stored electronically

Those principles relevant to paper records will apply to those pupil records stored electronically. School information management systems may incorporate features to enable elements of the electronic pupil record to be deleted in accordance with retention schedules, whilst the remainder of the record remains intact.

Storage and Security

All pupil records and associated information should be stored securely to maintain confidentiality whilst keeping information accessible to those authorised to see it. Electronic records should have appropriate security and access controls in place; equally paper records should be kept in lockable storage areas with restricted access. Not everyone in a school has a need to access all of the information held about a pupil; this is particularly relevant to child protection information. [see also the section on Information Security in this toolkit]

Transferring Pupil Records

It is vital to ensure swift transfers of information to the new school to ensure appropriate decisions can be made regarding a pupil, using relevant and accurate information.

Weeding

The pupil record should not be weeded before transfer, unless any duplicates or records with a short retention period have been included; these can be removed and securely destroyed.

Transfer Process

The following should be transferred to the next school within 15 school days of receipt of confirmation that a pupil is registered at another school:

- Common Transfer File (CTF) from the School Information Management System via the school2school system when used
- Any elements of the Pupil Record, held in any format, not transferred as part of the CTF
- SEN or other support service information, including behaviour, as only limited information may be included in the CTF
- Child Protection information; this must be sent as soon as possible by the Designated Safeguarding Lead (DSL) or a member of their team to their equivalent at the new school.

Schools must ensure the information is kept secure and traceable during transfer:

- Records can be delivered or collected in person, with signed confirmation for tracking purposes
- Pupil Records should not be sent by post. If the use of post is absolutely necessary, they should be sent by 'Special Delivery Guaranteed' or via a reputable and secure courier to a pre-informed named contact, along with a list of the enclosed files. The new school should sign a copy of the list to confirm receipt of the files and securely return to the previous school
- If held electronically, records may be sent to a named contact via secure encrypted e-mail, or other secure transfer method.

978-1-9161239-1-5

If the pupil is transferring to an independent school or a post-16 establishment, the existing school should transfer copies of relevant information only and retain the original full record as the last known school.

If a request is received to transfer the Pupil Record or other information about a pupil to a school outside of the European Union (EU), schools should contact the Local Authority or their Data Protection Officer for further advice.

Retention and Disposal

Retention - Transferring school

Responsibility for maintaining the pupil record passes to the next school. Schools may wish to retain the information about the pupil for a short period to allow for any queries or reports to be completed or where linked records in the school information management system have not yet reached the end of their retention period and deleting would cause problems.

Certain elements of the record may need to be retained for longer, for example if litigation is pending, or for transfer to the Local Record Office, in accordance with the Retention Schedule.

Whilst the Independent Inquiry into Child Sexual Abuse (IICSA) is ongoing, it is an offence to destroy any records relating to the Inquiry. It is likely, at the conclusion of the inquiry, that an indication will be given regarding appropriate retention periods for child protection records. More information can be found on the IICSA website.
Schools from which a pupil transfers should consider retaining a copy of the child protection file.

Retention – Last known school

The last known or final school is responsible for retaining the Pupil Record. The school is the final or last known school if:

- A secondary phase and the pupil left at 16 years old or for post-16 or independent education, or;
- It is a school at any point and the pupil left for elective home education, they are missing from education or have left the UK.

The Pupil Record should be retained as a whole for 25 years from the date of birth of the pupil, after which time, if no longer required, it can be deleted or destroyed. SEN and other support service records can be retained for a longer period of 31 years to enable defence in a "failure to provide a sufficient education" case.

If a school wishes to retain data for analysis or statistical purposes, it should be done in an anonymised fashion.

Disposal

Pupil records will contain personal and confidential information and so must be destroyed securely. Electronic copies must be securely deleted and hard copies disposed of as confidential waste. Please see the section on Safe disposal of records for further information.

Acknowledgements

Original content by:

Anthony Sawyer	Herefordshire Public Services
Joseph Bartoletti	Middlesbrough Council

Amendments and additions made by the following as part of the 2018 review:

Lizi Bird	Solihull Metropolitan Borough Council
Andrea Binding	Somerset County Council
Natalie Fear	One West, Bath and North East Somerset Council

Information Audits

1. What is an information audit?

An information audit is typically a record of the following:

- What information is retained
- Why information is retained
- What type of information it is
- How information is processed and shared
- Where information is stored
- What the relevant retention period is
- Who the 'responsible owners' or day-to-day users are

Note: you can expand on the audit and tailor it to your school, for example you may want to combine this with data protection impact assessment records and information sharing agreements.

An information audit should capture all information held, regardless of its form. You should consider:

- Paper documents and records
- Electronic documents and records
- Databases (proprietary or developed in-house)
- Microfilm/microfiche
- Sound recordings
- Video/photographic records (including those records taken on traditional magnetic tape and photographic paper but also, increasingly, digital sound, video and photo files)
- Hybrid files
- Knowledge
- Apps and portals

The information audit is designed to help organisations complete an information asset register. The terminology grows out of the concept of "knowledge management" which involves the capture of knowledge in whatever form it is held, including encouraging people to document the information they would previously have held in their heads.

It is now generally accepted that information is an organisation's greatest asset and that it should be managed in the same way as the organisation's more tangible assets such as staff, buildings and money.

Effective Information Management is about getting the right information to the right people at the right time and an information audit is key to achieving this.

2. What are the benefits of the information audit?

The information audit is designed to allow organisations to discover the information they are creating, holding, receiving and using, and therefore to manage that information in order to get the most effective business use from it. For a school, the concept is much more concerned with accessibility of information. The information audit allows the school to identify the personal information it creates and stores to facilitate correct management under the Data Protection Act (DPA) 2018 , the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

The following are all benefits to maintaining an information audit:

- It saves time - an information audit can be used as a quick point of reference for all staff; it ensures information can be easily located on a daily basis. This may also be useful for new starters or in the event of temporary cover arrangements.
- It avoids duplication – duplicating information is unnecessary, it adds to workloads and takes up unnecessary storage space which can be costly. Duplicating personal data would be a breach of the Data Protection Act 2018 as personal data must not be excessive. Identifying where the principal copy of a piece of information is held means that individual members of staff do not need to hold their own copy.
- It helps ensure accuracy of information – having a detailed record of information improves how you manage version control and therefore the likelihood that you are working from the most up-to-date version.
- Compliance with the Data Protection Act– individuals have numerous rights under the DPA in relation to their personal information. Whether you are dealing with a request to access information or an erasure request, the first step is identifying whether the information is held and where. If you don't maintain a record of processing, information may be missed and you could risk ICO enforcement.

978-1-9161239-1-5

The general timescale for dealing with requests under the DPA is one calendar month. Knowing where to locate information and identify if it has been shared with third parties can help save crucial time.

- Development of Record of Processing Activities (RoPA) – the information collected as part of the information audit can be included in the RoPA which a school develops.
- It assists the Data Protection Officer – the Data Protection Officer needs an overview of what personal information is held and how it is handled.
- Compliance with the Freedom of Information (FoI) Act 2000 – as public sector bodies, schools are obligated to provide certain information within 20 school days or 60 working days whichever is the shorter. Knowing what is held and where to locate information is an essential first step. Wrongly refusing a request or non-compliance with the statutory timescales could lead to ICO enforcement action.
- Identification of information which has passed its retention date – storing information can be costly regardless of whether it is physical or electronic. Significant savings can be made by ensuring that the relevant retention periods are identified and complied with. Applying retention periods also reduces the risk of not complying with the Data Protection Act 2018, GDPR or the Freedom of Information Act 2000. Finding information and preparing it in response to a request is much more difficult if there is a need to sort through significant quantities of information which should have been disposed of.
- It improves your ability to make the right decisions – schools deal with sensitive information on a daily basis. When making any decision in relation to the care of a child it is essential you consider all the relevant details, whether it is medical or otherwise.
- It reduces the possibility of an information security breach – names change, addresses change and family relationships change. Knowing where to locate the correct up-to-date information is essential. It reduces the risk of a breach which helps prevent unnecessary distress and the likelihood of your school facing ICO enforcement action and/or legal claims.
- It supports accountability and transparency - which is increasingly important under GDPR requirements.

3. How to complete an information audit

The information audit works on the premise that all information is created for a purpose (business need) and the information created and stored is to support that business need. The audit works through a work-flow process identifying which information is created at which point in the process, what it is used for, for how long it is needed, whether or not it should be captured as part of the core record of the school (i.e. whether it is a working document or a final policy or report) and whether it needs to be protectively marked.

The information audit can be conducted in a number of ways.There are two sample templates which are available to download on the IRMS web pages with a toolkit.

It's important that:

- you involve senior management with the audit at an early stage to ensure that they are engaged with the process and are prepared to give staff the support they need; all relevant staff are involved in the process and that they are given as much direction as possible about how to complete the audit.
- you let staff know what it is you're doing and why, even if you decide to send out templates for completion. After all, they work with the information and are best placed to identify it and any requirements. It also helps senior management and staff to understand their information responsibilities and should help ensure that the templates are completed and returned on time.

Once this process has been completed, the information audit should contain: a list of business needs; the kind of information created to meet that business need; the format in which it is stored; details on how long it needs to be kept; core records status and; any protective marking. The information audit should also contain where the information is collected from, who it is shared with and if consent is needed and how it is obtained.

Information Audits Continued

Once the information audit has been completed, consultation with the staff actually involved in the processes needs to take place in order to ensure that the audit is an accurate reflection of practice. At this point some negotiation may need to take place if there are any anomalies. The purpose of the information audit is to identify where processes can be improved, not merely to document what happens at present.

Once the information audit is felt to be accurate then the information asset register and/or the RoPA can be agreed. This enables all members of staff to see what information is created, by which business process, where it should be filed, and how it should be managed. This helps support legal compliance and business continuity by identifying any risks and mitigations around the management of sensitive information.

The results of the information audit should be presented to senior managers and the governing authority for comments and final approval. This will provide the audit with senior endorsement.

Finally, any information audit is a snapshot in time and only as good as the information provided by those taking part. In order for information systems to be kept up-to-date (including capturing information created by new and developing technologies and to take account of new functions and legislation) the audit results should be regularly reviewed and updated.

Acknowledgements

Original content developed by:

Craig Ferguson	Warwickshire County Council
Suzy Taylor	New College Durham
Keith Batchelor	Batchelor Associates

Minor amendments made at time of 2015 review.

The current version (including the template spreadsheets) was created as part of the 2018 review

Sinead Booth	Derby City Council
Catrina Finch	City of Wolverhampton Council

978-1-9161239-1-5

Management & Monitoring of Electronic Communications

Introduction
These guidelines have been developed to provide information about electronic communications best practice,and will hopefully help you balance staff and student privacy with the oversight necessary to ensure your safeguarding obligations are maintained.

The sections are:

- E-mail
- Messaging and Discussion Tools
- Monitoring staff and student use
- Essential Resources (including relevant legislation)
- What you need to know about Social Media

All electronic communications, whilst they are held, are disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an e-mail, an Instant Message (IM), a text, or on a message board, could potentially be made public. Electronic communications are very easy to copy and transmit and although you may have deleted your copy the recipients may not. Because of this they can form part of your records, commit you to contracts and expose your school to risk if used badly.

E-mail

Watch your language
As communicating by e-mail is quick and easy, the language in which e-mail is written is often less formal and more open to misinterpretation. Use spell-check and consider the tone of your wording.

Choose your recipients
Check the recipients are appropriate and typed correctly. Consider using role-based shared mailboxes (e.g. senco@schoolname.region.sch.uk / head@academy.org.uk), ensuring you carefully control who has access to any accounts.

Consider turning off the 'auto-complete' feature in the 'To' box as staff could easily send an e-mail to the wrong address.

Ensure that Bcc is used where appropriate to avoid the unauthorised disclosure of e-mail addresses of intended recipients. The ICO has taken enforcement action in cases where Bcc has not been used in sensitive cases.

Secure your data
The consequences of an e-mail containing sensitive information being sent to an unauthorised person can result in a fine of up to 20 million euros (or equivalent in sterling) or restrictions on processing from the Information Commissioner, along with adverse publicity for your school. Confidential or sensitive information should be sent by a secure encrypted e-mail or data transfer system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

Secure your devices
Did you know that e-mail Apps on mobile phones are usually unprotected? Did you know that, by default, Outlook will download the entire contents of a person's mailbox on a personal device (which can be easily accessed)?

If members of staff access school e-mails on personal devices, the school's IT support provider should be contacted for help with configuring the device and check for encryption, as well as ensuring that all devices require a suitable password for access. The key is to engage with your IT support provider who will be able to advise accordingly.

You could advise staff to only access work e-mail via the internet as the web client does not save data locally.

Management & Monitoring of Electronic Communications Continued

It's not a filing system

E-mail systems are commonly used to store information which should be stored somewhere else. E-mails and attachments should be saved into any appropriate electronic filing system or printed out and placed on paper files.

Where the text of the e-mail adds to the context or value of the attached documents it may be necessary to keep the whole e-mail. The best way to do this, and retain information which makes up the audit trail, is to save the e-mail in .msg format. Where you just want recipients to read a document, consider sending a link to the documents rather than attaching them.

How long do we keep e-mails?

E-mail is a communications tool, and e-mail applications are not designed for keeping e-mail as a record. E-mail that needs to be kept should be identified by content, for example:

- Does it form part of a pupil record?
- Is it part of a contract?
- Does it relate to an employee?

The retention for keeping these e-mails will then correspond with the types of records found in the Retention Schedule for schools below. These e-mails may need to be saved into an appropriate electronic filing system or printed out and placed on paper files. Similarly, information contained within these e-mails should be recorded in the appropriate place (e.g. the MIS or behaviour management system). Once this is done the original could be deleted.

Consider implementing an electronic rule whereby e-mails in inboxes are automatically deleted after a period of time, assuming they have been filed away. This will assist greatly in reducing the amount of information potentially disclosable in the event that a subject access request is received. Consider implementing procedures for the management of inboxes of staff who have left the organisation.

Limiting the information which is retained will also mitigate the school's liability in the event of a breach and will reduce the amount of electronic storage required.

Do you want a disclaimer?

Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient. Typically, disclaimers cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and that any views or opinions of the sender are not necessarily those of the school. There is some debate about how enforceable disclaimers are but they can help clarify the school's position in relation to the information being e-mailed.

Look out for Phishing!

Make sure staff are aware of the dangers of providing information over e-mail. Never provide passwords or personal data, or click on a link in an e-mail without verifying its source. Ask your IT department to provide advice.

Messaging: Texts, Instant Messaging

Text messaging and IM applications provide a quick, efficient way of communicating with individuals or groups.

These methods are largely suited to brief, informal messages; more formal conversations may be better suited to e-mail, telephone or delivered face-to-face. Avoid sending and posting sensitive/personal data as these systems may not be as secure as e-mail.

Consider your audience – it may be necessary for a message to be sent to an individual or a group of people but bear in mind that not everyone may have access to these tools and may not have given permission for their contact details to be used in this way. It may also create privacy issues if third parties are able to read messages not intended for them.

Internal Discussion Boards and Forums

Internal discussion boards and forums (e.g. Intranets, Microsoft Teams etc.) provide flexibility for collaboration in the workplace. They can also be very informal and are essentially public within the organisation, although some functionality can be shared with external parties and because of this they should never be used to share confidential or personal information.

978-1-9161239-1-5

Always ensure that staff or students that use these groups and spaces are aware of exactly who will see any information posted.

Any recorded information is subject to the same Data Protection and Freedom of Information legislation, regardless of format, therefore it would be advisable to only use these methods of communication to transmit information which you would be content to publish, that is to say; low risk information due to the lack of effective security and assurance.

Records Management

Content created and shared by messaging and discussion forums should be regarded as ephemeral and temporary. If the content subsequently becomes important (and is something that needs to be retained as a formal record, for example in a safeguarding case file), then it should be copied and moved into your filing system, either by saving it in a readable electronic format, printing it out or taking a screenshot. Whilst content does exist though, it is subject to both FoI and DPA.

Monitoring Staff and Student Use

Monitoring student and staff use of communications and the internet is a balance between a school's Safeguarding and PREVENT obligations and the user's right to privacy. It will be important to have a policy on this so you can demonstrate what you intend to do and to justify this in relation to your legal obligations.

An employer can monitor the use and content of staff communications provided it has informed members of staff that it may do so. If you intend to do this you will need to be able to prove that you have made staff aware that this may happen. You will need to have a policy and provide staff with advice on how you expect them to use systems such as e-mail, telephone, other messaging systems and the Internet (including Social Media).

Ensure you make a decision about how your IT provider logs people's use of your e-mail and internet, that the logging is an appropriate record, and that it suits your policy.

You should document your decisions as a retention period (see below).

Where third party support has access to logs (remote support purposes, etc.) then you need to establish how long they, as a data processor, retain any information which may contain personal information. You should instruct the third party about the retention period based on the school's requirements.

The Information Commissioner's Employment Practices Code (https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf) is an excellent resource to use when considering this area.

Legislation

- General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Defamation Act 2013
- Privacy and Electronic Communications Regulations 2003
- Counter Terrorism and Security Act 2015
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Acknowledgements

Original content developed for the 2018 revision by:

Claire Jurczuk	Department for Education
Tony Sheppard	GDPR in Schools
Suzy Taylor	New College Durham
Alison Tennant	Liverpool Diocesan Schools Trust

What You Need to Know About Social Media

Social Media can be used as a multi-use communication tool

Social Media forms a range of versatile tools that can be used in several ways. As a communication tool it can broadcast information, enabling a quick way to share information about the school in the form of text, pictures, video and/or audio. It can be used to have direct communications with stakeholders on a one-to-one, one-to-many or many-to-many basis, or it can make use of provided information to see who the school is engaging with.

The school must ensure that staff contributors maintain the school's standards for written communications on Social Media platforms. Changes to Social Media tools are fast-paced and so it is not always possible to give consistent instructions for certain tasks. There are several organisations that can support you with understanding how to set up and make the most of Social Media tools, usually with a strong emphasis on the role safeguarding plays with these tools.

Use of Social Media may require a risk assessment

Prior to implementing Social Media, staff must think about information security when they are sending or replying to messages/posts. Use of Social Media should follow protocols and procedures established by the school to ensure consistent use of Social Media and that staff do not release information inappropriately or illegally.

Schools using social media will need to establish what purpose they are using it for, the lawful basis as part of it, what data/information they will process, how they will uphold any of the rights of data subjects, and the retention periods involved. This is usually completed as part of a Data Protection Impact Assessment. Depending on how the school is planning to use Social Media tools, it may opt to complete an assessment, one per tool or bring several together based on how data flows through them (e.g. a blog post which may be tweeted and then finally published on Facebook, but is actually part of a single data flow).

Social Media is not always a secure and private platform

Social Media tools have a range of settings for both security and access to published posts/comments. This needs to be taken into consideration when publishing information and controlling who has access to it. Confidential or sensitive information should never be put online or shared via direct contact on Social Media. Where images, names of individuals or other personal data is used schools must ensure that they have a lawful basis for doing so.

Where this involves consent from the parents/children, the consent should be clear and unambiguous, including where the information will be shared and for how long. Records of consent should be kept with other records for the individuals involved where possible, but access must be provided for those that require it as part of day-to-day operations. It is important for parents and students to understand that, when giving their consent, the school cannot control the re-posting of information.

See also: https://www.saferinternet.org.uk/advice-centre/social-media-guides

Social Media posts vary in their retention

Social Media tools vary in their retention periods. When signing up for any tool the school needs to ensure that users are aware of these retention periods and ensure that it checks on a regular basis for changes. Where the retention period is longer than that set out as part of standard school policies, processes must be in place to remove any posts or comments, or to publish this fact within the Retention Schedule. Where posts include items which are hard to clearly index/search (e.g. images, video or audio), then a content register may be needed to manage when items have been shared, when they were shared, who it was in reference to, etc.

Social Media posts and messages don't necessarily delete immediately

Posts and messages can remain on the Social Media network for a period after the school has deleted them. Once messages have been posted they may be shared,

978-1-9161239-1-5

liked and commented on (in ways not originally intended). If so, there will still be copies in existence and if the recipient saves an image/screenshot they will have copies that can be distributed. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 2018 – they will also form part of the child or subject's digital footprint - clear and unambiguous consent is therefore key.

Social Media is disclosable under the access to information regimes

Both the Freedom of Information Act 2000 and Data Protection Act 2018 provide regimes for access to information based on specific requests. When completing risk assessments for publishing personal data this must be considered as part of enabling the rights of data subjects. FoI legislation also mandates that anything published as publicly accessible is potentially disclosable (subject to exemptions), either at the time or as part of any request.

Do staff and governors need another account for work?

In the same manner that using personal e-mail accounts for work means that they will be subject to FoI requests, the same applies for Social Media accounts. It is recommended, on safeguarding grounds, that dedicated work accounts are used and managed by the school. Any official school account should be tied to school e-mail addresses, and ensure that there is transparency within the school on who has access to these accounts.

Creating a Social Media account

Here are some steps to consider when creating a Social Media account. Please note that these guides are generic and are based on actions at the time of writing. Social Media tools change at a fast pace and you should always check with the provider for specific guidance for use within education, or check with organisations such as the UK Safer Internet Centre or ChildNet.

Creating a Facebook account

- Go to www.facebook.com
- Enter your name, e-mail or mobile phone number, password, date of birth and gender
- Click Create an Account
- To finish creating your account, you need to confirm your e-mail

Creating a class page/group on Facebook

Facebook really has two options to use when setting up a classroom account; you can create either a page or a group.

Pages are public for everyone to see, like, and comment on. There is the capability to block specific Facebook users if there are issues, but in general it is a very open platform. Individuals create the page through your personal account, but that doesn't mean followers can see the creator's personal posts.

Groups can be made private or public. They can even be made "secret" so that invitations can be sent just to the parents of a particular class You should not send personal friend requests when setting up groups; invite them to your page with a link by copying it into an e-mail.

Creating a Twitter account

Once you are on the Twitter homepage, enter your full name, e-mail address and password to create your account. Click on Sign up for Twitter and, on the next page, Twitter will use your name as your username if it's available (if you want to change this then do so at this stage). Click on create my account. Twitter will offer a few recommended accounts to follow - you can simply close this window, as my recommendation would be to only follow those Twitter accounts which make sense – and are relevant - to you. You will receive an e-mail from the Twitter verification team, click on the link in the e-mail to verify your account. Do remember to do this as it is an important step. Once you have verified your account, you will be taken to the Twitter home page and you will be logged into your account.

What You Need to Know About Social Media Continued

Creating and Sending messages/posts

Here are some steps to consider when sending messages and posting:

- Do you need to send this message/post?
- Do you need to communicate via Social Media, or would it be more appropriate to telephone or speak with someone face-to-face?
- Ensure that the messages/posts are clearly written
- Do not use text language or informal language in school messages/posts
- Always sign off with a name (and school contact details - never personal details)
- Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond
- Never write whole messages/posts in capital letters as this can be interpreted as shouting
- Always spell check messages/posts before you send them.

Sending attachments

Sending attachments on Social Media should be avoided; you should not be sending content to parents etc. via this platform. If they want to receive content, then they should make a request in person at the school or via authorised means for it to be processed. This ensures that compliance with data protection legislation is followed, as well as ensuring safeguarding issues are considered.

Broadcasting Information

Where information is broadcast across Social Media, a record of content/audience/information may be recorded. This is both good practice for ensuring a 'draft' is clearly written and recorded, but also allows the school to monitor what information has been shared and about whom.

Cascading Information

Where information is being re-broadcast/cascaded (e.g. a share or a RT) then it is good practice to still record this in a log. In instances where a data subject linked to the school has been re-broadcast it is still affected by both FoI and DPA access regimes.

Where posts are automatically cascaded between different social networks the security implications need to be considered to ensure that:

a) Only the right level of access is in place, ensuring that personal details from one platform do not 'leak' into another platform without your permission;
b) Any permissions or restrictions on sharing information on particular platforms are taken into consideration (consent records are key for this as some data subjects may not consent to information going onto particular Social Media platforms), and;
c) You are aware of any differences in retention periods between platforms.

Statistical Information

As more schools become media and marketing savvy, reviewing the statistics of Social Media tools is increasing. Generally, these hold little direct information about individuals, but where it is recorded then data minimisation principles need to apply.

Marketing

Where information is broadcast across Social Media in an indirect manner it is generally accessed by those who have chosen to view and access the information. Where people have 'subscribed' to follow anything broadcast by the school then a clear record of that subscription is needed. In the same way that e-mails are subject to Privacy and Electronic Communications Regulations 2003, Social Media tools also fall under this umbrella.

Managing Your Inbox

This section contains some hints and tips about how to manage incoming messages and posts. Remember that this depends on your expected use of each platform. Where you rely on any tools as part of early contact of incidents, you need to make sure it is readily monitored and is part of a range of controls you have in place.

978-1-9161239-1-5

Manage interruptions

Incoming notifications can be an irritating distraction. The following tips can help manage the interruptions:

- Turn off any alert informing you of a notification;
- Plan times to check notifications into the day;
- Only respond to posts and messages during school working hours. If you respond out of hours recipients will begin to expect a reply whenever they send a message which could cause issues and unrealistic expectations.

Manage content

Where important information is relayed to the school due to any incidents or early notifications from parents/stakeholders, a permanent record should be recorded in the appropriate system, including details of the original source (e.g. Direct Message from Twitter). This not only allows you to manage your records but also makes access to the information more appropriate for relevant staff/individuals.

Acknowledgements

Original content developed for the 2018 revision of the toolkit by

Tony Sheppard GDPR in Schools
Becky Taylor Acorn Trust

Information Security, Business Continuity and Digital Continuity

Introduction
These guidelines have been developed to provide information on how to ensure that the school's management of information and records complies with your legal obligations under Data Protection law and allows you to recover your records following a security incident.

The sections are:

- Information Security
- Business Continuity
- Data Breach Management
- Essential Resources and Legislation

The requirement for information security within the General Data Protection Regulation (GDPR) is that the school's use of data must ensure "appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

When considering the appropriate level of security for the school's information and records, factors will include the risk appetite of the governing body, and any relevant policies your IT provider or governing body already has. There are tools and standards for assessing information security maturity. These are included at the end of this guide.

Information Security
Schools must have controls in place to ensure the confidentiality, integrity and availability of the important data they process. These include:

Access Controls and Permissions
A policy, with associated procedures, must be in place to manage access to systems and records. This should include limits on how users access the resources, which user actions can be performed, and what resources users can access. Records should be made of what level of access is granted and retained as part of 'new starter/change of role' records, so that access can also be correctly updated when staff leave or change roles. It should also detail who is able to authorise requests to change people's permissions.

Where individuals are given access to personal or sensitive data, additional training should be provided to ensure that they are aware of the increased risks, responsibilities (including confidentiality responsibilities), and the consequences of unauthorised access.

Staff and students must be required by the system to maintain a strong password, which must be changed as appropriate, depending on the various systems involved. Guidance is available from the Information Commissioner's Office (ICO) (see section 5 of this guide).

Recent court and ICO decisions concerning employees' unauthorised access to sensitive information - and subsequent criminal actions in publicly posting the information - highlight the need for schools to be able to maintain audit trails of who has access to information, as well as ensuring that appropriate security measures, including supervision, are in place.

As the Data Controller, your school should have Data Sharing Agreements in place with Data Processors and/or other 3rd parties you share data with (including Joint Data Controllers). These will include information about relevant Access Controls and Permissions, including references to sub-Data Processors. Seek guidance from the school's Data Protection Officer (DPO) where appropriate.

Physical Security
Physical access to records should be restricted. Key IT Infrastructure, servers, certain desktop/laptop devices and paper records must be kept in restricted environments, or areas with controlled access.

Clear policies, which are readily understood by staff, must be in place governing any removal of hard copy documents off site. Whilst the removal of hard copy documents is not to be encouraged, there may be occasions when it is necessary, in which case there should be a process for logging it.

978-1-9161239-1-5

There should also be guidelines for staff regarding locking documents in the boot of a car if the information is to be unattended for a period of time, when they must ensure that information is kept on their person, not leaving documentation in a vehicle overnight etc.

Ideally documents should be logged as having been taken out and must be returned to school at the earliest possible opportunity. As with any policy, it is essential that these messages are reinforced at appropriate opportunities with all staff, beyond the point of induction.

Staff should be particularly alert to the need to shred trip packs upon return to school, particularly since they will contain particularly sensitive health and behavioural data of the pupils concerned.

In school, filing cabinets containing personal information must be locked as should any records storage areas. This will be paramount in the case of safeguarding records maintained by the Designated Safeguarding Lead, but it will also apply to any class records maintained by staff within the classroom.

A record of files checked out from a central system must be maintained, logging their location. Access should also be logged in the same manner/same record as for digital access to records and resources, where appropriate (e.g. Pupil Records Archive).

A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information - it involves the removal of the physical records which contain sensitive personal information to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all its contents.

Documents containing personal data must be collected immediately from printers and not left on photocopiers. Schools should ideally require staff to log on to a printer or copier to obtain their prints, thus reducing the risk of data breaches. However, staff must be aware of the possibility of documents being left on the scanner area of the copier, or documents being produced in the event of a paper jam.

Where physical access cannot be fully restricted then security measure should be taken to deal with possible removal of devices, including physical restraints (locks) and encryption.

Remote Access

A remote access solution allows access to any files, databases or information systems on the network whilst the member of staff or student is not physically located in the school. It should have strong security controls put in place and regular reviews to ensure that it is still secure.

Schools should decide what restrictions are necessary to prevent information or records being downloaded, transferred or printed whilst the user is offsite. Devices connecting to any remote access system should be considered as part of the network and all appropriate security measures should be taken to protect the network and all systems from possible attacks from that device or any other source.

Bring your Own Device (BYOD)

In environments where BYOD is permitted, policies need to be in place to regulate the usage of such devices. It is best practice to ensure staff and students can't connect devices directly to the network but have to register those devices first. Devices can be segregated from sections of the network and access to key resources better controlled and logged.

Where personal data is stored on this device (via e-mail, access to local copies of cloud storage, downloaded files, etc.) then suitable controls should be put in to place to remove it, even to the point of remotely wiping any device. Where devices cannot be remotely wiped, they should automatically wipe if repeated, unauthorised attempts to access are made. Access on devices that are not encrypted should be restricted and documents must not be stored. Access should be through secure portals and carefully controlled, with guidelines to staff being reinforced to ensure that third parties cannot gain unauthorised access to information. This includes family members in the event that shared devices are used. Devices must be password protected.

Information Security, Business Continuity and Digital Continuity Continued

Software Management

The school should have a policy on patching (or updating) software (including firmware) to ensure bugs are fixed and any security vulnerabilities are addressed. This should be related to the school's risk appetite as patching early is generally more secure, but there is an increased likelihood of reliability issues due to bugs and potential compatibility issues. The school's IT provider should be able to make a recommendation based on best practice.

Anti-virus and anti-malware software require regular updates to provide appropriate protection, and this should happen in an automated fashion, with exceptions and issues notified to designated contacts. This enables key staff to be aware of any infections or risks to data within the school at the earliest possible opportunity, therefore minimising risk to data. It is also recommended that you undertake a review of protection on an annual basis to ensure protection is still fit for purpose.

Software is protected by The Copyright Designs and Patents Act and gives rights of control in relation to the use and distribution of software to the software company. The licence agreement at point of purchase covers copyright and outlines how the software can be used; failure to comply with the licence and UK legislation can result in legal action.

Schools should actively engage suppliers and renew maintenance agreements to ensure that they are running the latest versions of software. More often than not, exploits (methods used by hackers to gain unauthorised access) are patched/fixed in the operating system, but outdated legacy applications are not maintained so the threat remains. Enforcement action has been taken against organisations where breaches have occurred due to known vulnerabilities in the software and remedial action has not been taken.

Operations Management

Security incidents and faults in the system can involve disclosure, alteration or loss of information with the potential of a data breach if personal data is involved. Contingency planning for such events should form part of the school's critical incident management policy/business continuity planning. It is important that any incident is reported immediately to the Head Teacher and Data Protection Officer (DPO) so that containment and investigation can begin (see later section on data breaches).

The response to a security incident must include securing evidence of breaches and evidence of any weakness in existing security arrangements.

Systems Management

To help understand and manage the school's information assets (these are usually systems in which data is held e.g. the MIS system, the HR and Payroll system, student files, etc.) both an Information Asset Register (IAR) and a Record of Processing Activity (RoPA) should be produced. It is important that a school knows and fully understands the information it holds and how that information is used, so that appropriate security and protection can be put in place, as per Article 30 of GDPR and steps 2-5 of the DfE Data Protection Toolkit for Schools.

Organisations with 250 or more employees must document all their processing activities (RoPA).
There is a limited exemption for small and medium-sized organisations that employ fewer than 250 people – they need only document processing activities that meet the following criteria:

- They are not occasional (e.g. are more than just a one-off occurrence, or something they do rarely);
- They are likely to result in a risk to the rights and freedoms of individuals (e.g. something that might be intrusive or which might adversely affect individuals);
- They involve special category data or criminal conviction and offence data (as defined by Articles 9 and 10 of the GDPR).

Within schools, this will cover a significant number of areas and an initial review will be needed to identify what data is being used anyway.

978-1-9161239-1-5

For further information about information audits see the section earlier in this toolkit.

For further information about information asset registers and retention schedules see the section later on in this guide.

An Information Asset Owner (IAO) needs to be identified for each asset or group of assets. The IAO has responsibility to ensure that the asset is managed appropriately, meets the requirements of the school and monitors risks and opportunities.

Remember Information Assets can be hard copy files as well as IT systems or network shares.

The ICO mentions that compiling your RoPA should not be a one-off activity and the document needs to be regularly reviewed.

Planning

The GDPR requires schools to undertake a Data Protection Impact Assessment (DPIA) for a new project or system when the type of processing is likely to result in high risk. This could be because you're using a new technology or biometric data, or because the data is related to children. Your DPIA will help you with identifying data protection risks and will support you in demonstrating compliance with data protection laws. It is recommended that you carry out a DPIA for any new project that involves using personal data.

If the school's DPIA identifies a high risk that cannot be mitigated, it must consult with the ICO. To conduct a DPIA you should speak to your Data Protection Officer.

When a new system is introduced, it is important to ensure that the development system, test system and associated data is kept separate from the live system and data; live data must not be used for testing or development. Where 'piloting' is needed to assess suitability, live data is frequently used, but schools need to remember to treat the system as if it was a full system and complete any risk management activities.

The school also needs to ensure that they do not forget to remove data at the end of an unsuccessful 'pilot'.

For further information about GDPR see the relevant section below.

Training

Staff, including governors and volunteers, should undergo regular training on the following:

- Data protection, including recognising what a subject access request is
- Correct use of devices and systems
- Information security
- Online safety
- Acceptable use of the school's IT facilities
- The school's procedures and protocols for sharing and disclosing personal data

Training is essential to establish a sound culture of good data protection practices. It should help to prevent data breaches and, in the event that a data breach occurs, it should help to mitigate any action taken by the ICO against the organisation. The ICO will inevitably be interested in what training employees have had when investigating any breach that is reported to it.

Network and Storage Management

Where schools make use of cloud storage instead of, or alongside, physical onsite servers, you should always ensure that the location of the cloud storage and the security offered is appropriate for the information and records stored.

Appropriate client software should be available to transfer data in a secure manner, and relevant licences should ensure that the correct level of service is used as sometimes the free version of an online service (file sharing service, survey provider) can be less secure than the business or premium version. Where files will be synced to local devices, access should, where possible, be controlled to ensure that it only syncs to agreed and encrypted devices.

Information Security, Business Continuity and Digital Continuity Continued

Schools should try to keep data in one place as much as possible – e.g. if Office 365 is the sharing platform, Google Drive should not be used as well.

The use of memory sticks and USB devices should be discouraged and, at a minimum, all should be encrypted.

Business Continuity

Business continuity planning includes all the steps and activities required to maintain operations in the event of a disaster or disruption. It is often made up of various activities including business impact and risk assessment, business continuity and disaster recovery.

Business Impact Analysis (BIA)

A Business Impact Analysis will enable you to identify what records are critical to the running of the school. You can then identify what systems and data are required to allow you to access and maintain these records. Your BIA will support you in planning the recovery of hard copy and electronic records that are critical to the operations of the school. Your IT provider should be able to work with you to identify critical IT systems and ensure that they are covered by effective backups.

A risk assessment should also be carried out which will identify the threats and vulnerabilities to the records you process. You should consider how resilient your systems are, as these will be critical in ensuring the school can still access important data.

The school should identify ways to protect school records in relation to the threats and vulnerabilities identified. These should focus on protecting the confidentiality, integrity and availability of your data whether held on a computer or in paper copy.

Remember that prevention of damage to paper records must be considered. Metal filing cabinets are a good first level barrier against fire and water. Store vital records with appropriate security, not on open shelves or on the floor. Ideally, consideration should be given to transferring paper records to electronic records where possible, with appropriate electronic backups in place.

Backup Strategy

The school's IT provider can help to decide a suitable schedule for IT backups, based on the outcome of the Business Impact Analysis, giving priority to vital systems. This will also ensure they are aware of the school's priorities when it comes to disaster recovery.

The school's disaster recovery plan should focus on the restoration of records to a usable state, whether held on a server or in a filing cabinet.

The plan should include an incident response team, detailing the job roles within the school that are required to work together in the event of a disaster. It is important that the school's DPO is involved in disaster response and knows when a breach needs to be reported to the ICO.

In addition to the plans for restoring your IT systems to business as usual, you will need to consider:

Who is responsible for liaising with the incident response team?

Remember if there has been a data breach, you will need to investigate and decide whether you need to report to the Information Commissioner's Office. If in doubt you should contact the ICO helpdesk for advice - 0303 123 1113 during office hours.

978-1-9161239-1-5

The need to ensure the school knows what it has lost

- How will it track down paper files that have been checked out?
- Does it have details of suppliers who may be able to recover important records that have been damaged?
- Are there any costs that might be associated with the restore? Has appropriate provision been made in the budget for this?
- Who is responsible for authorising the restoration of data? For example, the restoration of a MIS database may require multiple authorisations for the restoration to take place (i.e. both the Network Manager and the Data Manager have to agree to the restoration).

The disaster recovery plan should be tested to ensure that it can be trusted. For example, a simulation test for electronic records could involve restoring your MIS to a test environment.

Data Breach Management

As with all other organisations, schools have had to deal with data breaches in the past and have done so with a variety of methods which haven't always been consistent. The recent changes introduced by GDPR and the Data Protection Act 2018 have consolidated what should be done and this section reviews the approach to managing records around Data Breaches.

There are a range of methodologies for managing breaches, how investigations take place, language used for contacting data subjects, etc. The DfE has published a Data Protection Toolkit to help support schools and the ICO has also provided advice on reporting a Personal Data Breach (see section 5 for links), with a specific form to help organisations gather data should they need to report such a breach.

As part of Data Breach Management, the school will need quick access to key records. Ensuring your DPO and any Data Protection leads have access to this information is essential.

All breaches should be internally logged for a number of key areas.

- Data discovered/reported to the school (key for starting the 72-hour countdown)
- Review of breach – what impact it had (understanding whether it is a Personal Data Breach or not), including any commentary, category of data disclosed, number of records, etc.
- Records of any immediate actions (to close the breach/ minimise risk to individuals if needed)
- Resultant risk and subsequent report (if risk to individuals then report to ICO, if significant risk to individuals then report to data subjects too)
- Subsequent actions
- Status (not a breach, not a reportable breach, reported-ICO, reported-Data Subjects)
- Additional actions
- Completed

The ICO form allows you to record a lot more detailed information and there are a range of toolkits and compliance engines available to hold more detailed information or guide you through actions. Updates to guidance are published via the ICO and specific school guidance via the DfE on a regular basis. The school's DPO will help the school decide if a breach needs to be reported to the ICO.

Records on breaches and subsequent actions will need to be retained to show how the school has complied with legislation. These records should be kept according to your records retention schedules, which should specify that a record is retained until the students concerned would reach the age of 25. For data breaches relating to staff data the retention period would be 'current year + 6 years.

Information Security, Business Continuity and Digital Continuity Continued

For further information about data breaches see the section on GDPR below.

Essential Resources

From the ICO Website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

From the Government:

https://www.gov.uk/government/collections/statutory-guidance-schools

https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

Useful Standards and Models:

ISO27000 series – Information Security
https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
BS10008:2014 Evidential Weight and Legal Admissibility of Information Stored Electronically
ARMA GARP Maturity Model
https://en.wikipedia.org/wiki/Generally_Accepted_Recordkeeping_Principles
COBIT (IT Governance Framework)
http://www.isaca.org/cobit/pages/default.aspx

Relevant Legislation

General Data Protection Regulation
Data Protection Act 2018
Freedom of Information Act 2000
Human Rights Act 1998
Privacy and Electronic Communications Regulations 2003
Copyright Designs and Patents Act 1988

Acknowledgements

Original content for the 2018 revision of the toolkit developed by:

Romin Partnovia	EduGeek.net
Tony Sheppard	GDPR in Schools
Suzy Taylor	New College Durham
Alison Tennant	Liverpool Diocesan Schools Trust
Joel Thornton	The Little IT Company

978-1-9161239-1-5

Digital Continuity

The long-term preservation of digital records is more complex than the retention of physical records. A large number of organisations create data in electronic format which needs to be retained for longer than 7 years. If this data is not retained in accessible formats, the organisation will be unable to defend any legal challenge which may arise. In order to ensure that digital records are retained in a way that ensures they can be retrieved in an accessible format when they are required, all records which are required to be retained for longer than 6 years should be part of a digital continuity statement.

The average life of a computer system can be as little as 5 years, however, as digital continuity is resource intensive, only records which are required to be retained for 6 years (in line with the Limitation Act 1980) or longer should be subject to digital continuity statements.

The Purpose of Digital Continuity Statements

A digital continuity statement will not need to be applied to all the records created by the school. The Retention Schedule should indicate which records need to be subject to a digital continuity statement. Any record which needs to be preserved for longer than 6 years needs to be subject to a digital continuity statement.

Appropriate records need to be identified as early in their lifecycle as possible so that the relevant standards can be applied to them. Conversely, any records which do not need to be included in the policy should also be identified in the early part of the lifecycle. Digital continuity statements should only be applied to principal copy records.

Allocation of Resources

Responsibility for the management of the digital continuity strategy, including the completion of the digital continuity statements should rest with one named post holder. This will ensure that each information asset is "vetted" for inclusion in the strategy and that resources are not allocated to records which should not be included in the strategy.

Storage of Records

Where possible, records subject to a digital continuity statement should be "archived" to dedicated server space which is being backed up regularly.

Where this is not possible the records should be transferred to high quality CD/DVD, if they are to be included with paper documentation in a paper file, or onto an external hard drive which is clearly marked and stored appropriately. Records stored on these forms of storage media must be checked regularly for data degradation.

Flash drives (also known as memory sticks) must not be used to store any records which are subject to a digital continuity statement. This storage media is prone to corruption and can be easily lost or stolen.

Storage methods should be reviewed on a regular basis to ensure that new technology and storage methods are assessed, and where appropriate added to the digital continuity policy.

Migration of Electronic Data

Migration of electronic data must be considered where the data contained within the system is likely to be required for longer than the life of the system. Where possible, system specifications should state the accepted file formats for the storage of records within the system.

If data migration facilities are not included as part of the specification, then the system may have to be retained in its entirety for the whole retention period of the records it contains. This is not ideal as it may mean that members of staff have to look on a number of different systems to collate information on an individual or project.

Software formats should be reviewed on an annual basis to ensure usability and to avoid obsolescence.

Digital Continuity Continued

Degradation of Electronic Documents
In the same way as physical records can degrade if held in the wrong environmental conditions, electronic records can degrade or become corrupted. Whilst it is relatively easy to spot if physical records are becoming unusable, it is harder to identify whether an electronic record has become corrupted, or if the storage medium is becoming unstable.

When electronic records are transferred from the main system to an external storage device, the data should be backed up and two secure copies of the data should be made.
The data on the original device and the back-ups should be checked periodically to ensure that it is still accessible. Additional back-ups of the data should be made at least once a year and more frequently if appropriate.

Where possible, digital records should be archived within a current system. For example, a designated server where "archived" material is stored, or designated storage areas within collaborative working tools such as SharePoint.

Internationally Recognised File Formats
Records which are the subject of a digital continuity statement must be "archived" in one of the internationally recognised file formats.

Review of Digital Continuity Policy
The Digital Continuity Policy should be reviewed on a bi-annual (or more frequently if required) basis to ensure that the policy keeps pace with the development in technology.

Digital Continuity Strategy Statement
Each digital continuity statement should include the following information:

- Statement of business purpose and statutory requirements for keeping records
- The statement should contain a description of the business purpose for the information asset and any statutory requirements, including the retention period for the records. This should also include a brief description of the consequences of any data loss.

By doing this the records owner will be able to show why and for how long the information asset needs to be kept. As digital continuity can be resource intensive, it is important that the resources are allocated to the information assets which require them.

Names of the people/functions responsible for long term data preservation
The statement should name the post holder who holds responsibility for long-term data preservation, plus the post holder responsible for the information assets. The statement should be updated whenever there is a restructure which changes where the responsibility for long term data preservation is held.

If the responsibility is not clearly assigned there is the danger that it may disappear as part of a restructure process rather than be reassigned to a different post.

Description of the information assets to be covered by the digital preservation statement
A brief description of the information asset taken from the IAR.

Instructions for when the record needs to be captured into the approved file formats
The record may not need to be captured in to the approved file format at its creation. For example, an MSWord document need not be converted to portable document format (PDF) until it becomes semi-current. The digital preservation statement should identify when the electronic record needs to be converted to the long term-supported file formats identified above.

Workflow process diagrams can help identify the appropriate places for capture.

978-1-9161239-1-5

Description of the appropriate supported file formats for long term preservation

This should be agreed with the appropriate technical staff.

Retention of all software specification information and licence information

Where it is not possible for the data created by a bespoke computer system to be converted to the supported file formats, the system itself will need to be mothballed. The statement must contain a complete system specification for the software that has been used and any licence information which will allow the system to be retained in its entirety.

If this information is not retained it is possible that the data contained within the system may become inaccessible, with the result that the data is unusable with all the ensuing consequences.

Description of where the information asset is to be stored

Description of how access to the information asset is to be managed within the data security protocols

The data held for long term preservation must be accessible when required, but also must be protected against the standard information security requirements which are laid down for records within the authority. The statement must contain the policy for accessing the records and the information security requirements attached to the information assets.

Please note that this content has been included from the 2016 version of the IRMS Records Management Toolkit for Schools and has not been reviewed. The original section on Digital Continuity was created by the Editor.

Safe disposal of records which have reached the end of their retention period

Please be aware that under the terms of The Independent Inquiry into Child Sexual Abuse (IICSA) it is an offence to destroy any records that might be of relevance to the Inquiry . This overrides all business, statutory, regulatory or legal retention requirements, including data protection requirements and the data subject's right to erasure. It is anticipated that upon conclusion of the Inquiry, further guidance regarding retention will be published.

1. Managing Records Retention

The fifth data protection principle states that "Personal data must be kept for no longer than is necessary for the purpose for which it is processed" . Therefore, all records, in all formats, should be subject to an applicable retention period, as defined by business, statutory, regulatory, legal or historical requirements. All retention and disposal decisions should be documented in a Retention Schedule as part of the school's records management policy (see Retention Guidelines section).

Each school should have an officer designated as their school records manager, with responsibility for ensuring records are retained, reviewed and destroyed in accordance with requirements, and as soon as possible once their lifespan has expired. The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained for ongoing business or legal purposes.

All records in all formats must be assigned a retention period and disposal date, either upon creation or when they cease to be in active use, in accordance with the Retention Schedule or policy. A system should be implemented to routinely identify records as soon as they reach their disposal date. This may form part of an electronic record-keeping system or a manual system.

Disposal must be carried out in a timely manner to:

- Ensure compliance with business and legal retention requirements
- Improve the efficiency of the record keeping system
- Free up storage space
- Reduce associated storage and management costs

Destruction must include all backup and duplicate copies, in all formats. This is especially vital for personal information which may be kept in various hybrid record keeping systems.

2. Principles of Disposal

Schools must agree a standard policy and procedure for the safe disposal of records. This policy must be communicated to all employees and regularly reinforced to avoid any possible data breach. Furthermore, if retention periods are not complied with, material will still have to be provided if a Data Subject Access request or Freedom of Information request is received.

The disposal method must be applicable to the content and format of the information. Paper and electronic records should be disposed of separately, i.e. floppy disks, CDs, DVDs, tapes, USBs, etc. should not be put into confidential waste containers containing paper as they require different disposal methods and could damage shredding equipment.

Destruction must be undertaken in a way that preserves the confidentiality of the information and which makes it permanently unreadable or unable to be reconstructed or re-instated. Special care should be taken when destroying personal, sensitive or commercial information and confidentiality should be paramount at all stages of the process.

3. Destruction of Records by Type

3.1 Paper Records

All hard copies of official records and those containing personal data must be destroyed using confidential methods, rather than being placed in general waste bins or skips, which could result in a data breach. Specialist companies can provide confidential waste bins and other services to ensure records are disposed of in an appropriate way.

978-1-9161239-1-5

- Open confidential waste bins – this method is most suited to low-level administrative records, not containing sensitive personal data, which are not governed by a business or legal retention period, and which do not require full audit trails. Bins must be placed in areas where security and access are not compromised. They must not be placed in public areas, such as reception areas. They must be clearly labelled as 'confidential waste', with contents being shredded on a regular basis.
- Office shredding machines – these are not usually practical, due to limited capacity and inefficient use of staff time. Ideally, they should be restricted to small ad-hoc quantities and for highly sensitive and confidential documents that should be shredded immediately. Cross-cut or micro-shredders are preferential to strip-cut shredders as they produce much shorter length strips which ensures higher security levels. Controlled use of an office shredder may be the only option for schools with limited budgets who cannot afford to pay for a regular shredding service. A process needs to be agreed and followed in schools that are using a shredder to ensure that information security is maintained at all times.
- Secure shredding cabinets – these are available with or without in-built shredding mechanisms. They enable records to be held safely until removed for shredding or recycling. They must be locked and placed in a secure office location, with a tamper-proof post slot and should be emptied regularly.
- Confidential waste sacks – these are available from shredding contractors. Bags must be secured (e.g. zip tied) in situ, placed in a secure area whilst awaiting collection and a log created to identify how many bags are awaiting collection, as well as the contents of the bags.
- Shredding contractors – provide the most secure method of shredding. GDPR requires that a contract be in force between the data controller (the school) and the processor (the contractor) to ensure that they both understand their obligations, responsibilities and liabilities, even if the destruction is taking place on the school site.

The school will retain the responsibility of data controller, aswell as the liability for non-compliance caused by the contractor under GDPR. However, if the contractor breaches the terms of the contract or acts outside of the school's instructions, it will become liable under GDPR. It is therefore essential that schools check the terms of the contract and set out instructions in a Data Processing Agreement on how the school's data must be handled. It is recommended that schools check their insurance to ensure that they are not at undue risk and are adequately covered. For example, if a contractor disposed of confidential waste inappropriately, security was breached, or data was otherwise lost whilst in the care of the contractor.

Third party contractors should be certified to the following:

- BSEN15713 – secure destruction of confidential material
- BS7858 – staff security vetting
- ISO 9001 – service quality
- ISO 14001 – environmental management standard
- ISO 27001 – information security

Additionally, membership of the following organisations and associations are recommended:

- BSIA – British Security Industry Association
- FACT - Federation Against Copyright Theft
- FTA – Freight Transport Association
- FORS - Fleet Operator Recognition Scheme
- NAID – National Association for Information Destruction
- SafeContractor – health and safety assessment scheme
- UKSSA – UK Security Shredding Association

Third party contractors provide a short chain of custody, which significantly reduces the risk of a data breach. Accredited contractors will meet requirements for environmental conditions, the physical security of vehicles and facilities, and they will shred to a minimum of DIN3. Shredding contractors should be trained in the handling of confidential records. Their premises, policies, processes and accreditations should be regularly audited to ensure compliance to requirements.

Safe disposal of records which have reached the end of their retention period Continued

Whilst contractors with accreditation may have had DBS checks, schools should assess the level of risk in accordance with their staff supervision policies, in order to determine whether safeguarding requirements are met and whether full supervision is required.

Many contractors can provide both mobile on-site shredding and off-site shredding services. Mobile shredding services ensure that all material has left the premises shredded to approved standards. However, they also tend to be more expensive which means that schools are less likely to opt for them. The chain of custody and Certificate of Destruction mean that when an approved shredding contractor picks up the material and takes it offsite, all legal responsibility transfers from the school to the contractor. If the school has completed its GDPR due diligence on the shredding contractor, off-site shredding is just as secure and possibly more economical than mobile shredding.

Approved contractors should always provide a Certificate of Destruction, which should be retained with details of individual records destroyed. A secure area must be designated where records can be stored prior to shredding.

It is vital to ensure shredded material cannot be put back together. The European standard, DIN 32757, is the standard for paper shredding. There are six levels, ranging from DIN1 to DIN6. The higher the number the higher the standard of shredding and the smaller the shred size. DIN 1 - 2 provides the least level of security, with DIN 5 - 6 being used mainly by central government and the military. DIN 3 - 4 is recommended for public authority records, including school records.

3.2 Electronic and Other Media Records

Deletion of electronic records should be a managed and auditable process in the same manner as paper records. Records should be routinely identified for deletion and should be authorised by the relevant senior officer. Before deletion, it must be determined that all legal and business requirements have expired, and that there is no related litigation or investigation. Records must be securely deleted in accordance with the school's security policy. Processes must be in place to ensure that all backups and copies are included in the deletion process.

However, it is not always straightforward to delete information from electronic systems. If a system is not able to permanently and completely delete all electronic data, it should be 'put beyond use'. This means it should:

- Not be used for any decision making, or in a manner which affects an individual in any way
- Not be given to any other organisation
- Have appropriate technical and organisational security and access controls
- Be permanently deleted when this becomes technically possible

If information is 'put beyond use' the individual's Data Subject Access right is exempt . However, if such information is still held it may still need to be provided in response to a court order.

The method of deletion should be suitable to the type of information. The school's ICT department or IT provider should be able to advise on the most appropriate method. Common methods for deleting electronic records are:

- Deletion – this is the easiest and most appropriate method for non-confidential records. However, it is important to remember that deletion from a server may not be sufficient, as this only destroys access to the record - e-discovery and recovery tools will still be able to recover the information. To achieve full destruction, overwriting with random digital code may be more appropriate.
- Overwriting – this method makes e-discovery and recovery more difficult. It is recommended to overwrite using random digital code at least three times.
- Degaussing (magnetic media) – exposing magnetic media, such as tapes and floppy disks, to a magnetic field scrambles the data beyond use or re-instatement.

978-1-9161239-1-5

- Physical destruction of the storage media – physically destroying the media on which the information is stored is the most suitable method for portable media:
    - CDs/DVDs/Floppy Disks should be cut into pieces
    - Audio/Video Tapes and Fax Rolls should be dismantled and shredded
    - Hard Disks should be dismantled and sanded
    - USBs should be submerged in water and dismantled.

The ICO and National Cyber Security Centre (NCSC) make certain recommendations for organisations with regards to deleting, remarking or recycling IT equipment. In accordance with this it is recommended to use an IT asset disposal company that is fully certified with the industry body, the Asset Disposal Information Security Alliance (ADISA) .

4. Transfer of Information to Other Media

Where lengthy retention periods have been allocated to records, the school may wish to consider converting paper records to an alternative format, such as microfilm or digital media, e.g. scanning. The lifespan of the media, and the ability to migrate data where necessary, should always be considered.

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standardised fashion and to ensure the quality of the electronic version. Organisations must be able to evidence that the electronic version is a genuine copy of the original, and that the integrity of the data has not been compromised.

It is recommended that original versions of records be retained for up to six months after transfer to an alternative media, so as to provide adequate time in which any issues arising out of the data transfer process may be identified.

Specialist companies will transfer information to alternative media, including microfilming and scanning.

It is recommended that an external provider is used for any large-scale projects, as this is more cost effective and has integral quality assurance standards. However, when outsourcing it is essential to ensure that the contractor is GDPR compliant and conforms to all security and staff vetting requirements, and to have a Data Processing Agreement in place.

Reference should be made to British Standard 10008:2008 'Evidential weight and legal admissibility of electronic information' when preparing such procedures.

Please note that scanning has been approved under IICSA, providing effective quality assurance and data integrity standards have been met, which conform to BS 10008:2008.

5. Transfer of Records to the Local Record Office

Where records have been identified as being worthy of permanent preservation, arrangements should be made to transfer the records to the Local Record Office. This may be done during the records' active use, or once administrative use has concluded (depending on their condition) access requirements and advice from the Local Record Office. Once records have been transferred, they will continue to be managed in accordance with the Data Protection Act 2018 and the Freedom of Information Act 2000 and will be subject to any applicable closure periods.

The school should retain details of what has been transferred to the Local Record Office to enable their identification, if required for future use.

If a school chooses to keep their archive records on site for use with pupils and parents, they should contact the Local Record Office for specialist advice on storage and preservation requirements.

Details of records which should be transferred to the Local Record Office can be found in the Retention Guidelines section.

Safe disposal of records which have reached the end of their retention period Continued

6. Documenting of all Archiving, Destruction, Deletion and Digitisation of Records

To satisfy audit, accountability, legal and business needs, it is vital to keep a record of all archiving, destruction, deletion and digitisation. The Freedom of Information Act 2000 requires schools and Academies to maintain a list of records which have been destroyed and a record of who authorised their destruction.

The Freedom of Information Act 2000 states that, as a minimum, the school should be able to provide evidence that the destruction of records took place as part of a routine records management process. Schools must assess whether they are creating another piece of Personal Identifiable Information (PII) by maintaining a record of evidence, particularly if they are listing the names of the people whose records have been deleted.

A comprehensive records management policy and retention schedule will provide a detailed process to ultimately ensure that the records have been destroyed and should stand as the minimum required under the FoI Act.

A record should be retained of:

- File reference (or another unique identifier)
- File title (or brief description)
- Number of files or volumes
- Date range
- Reference to the applicable retention period
- The name of the authorising officer
- Date approved for disposal
- Date destroyed or deleted from system
- Method of disposal
- Place of disposal (whether on-site or off site by a contractor)
- Person(s) who undertook destruction

Sample appendices are provided below for the recording of all records destroyed or deleted, transferred to the Local Record Office or converted to an alternative media. These records should be retained permanently by the school for audit purposes.

Acknowledgements

Original contents developed by:

Sarah Graham	Information Governance Officer (Records Management) Newcastle City Council
Lia Lutfi	Birmingham City Council
Alison Marsh	Salford Royal NHS Foundation Trust

Amendments made as part of the 2018 review by:

Andrea Binding	Somerset County Council
Ciara Carroll	Cirrus Primary Academy Trust
Andy Crow	Chorus Advisers
Natalie Fear	One West, Bath and North East Somerset Council

978-1-9161239-1-5

Schedule of Records Destroyed/Deleted by [Name of School]

Unique Identifier	File Title/ Brief Description	Covering Dates	Quantity/ No. of Vols	Retention Policy Ref.	Authorising Officer	Date Approved for Disposal	Date Destroyed	Disposal Method	Place of Disposal	Destroying Officer/Contractor

Safe disposal of records which have reached the end of their retention period Continued

Schedule of Records Transferred by [Name of School] to [Name of Organisation/Local Record Office] for Permanent Preservation

Covering Dates	Unique Identifier	Title	Description	Quantity

On behalf of the school:

Signed: .....

Name (PRINT): .....

Job Title: .....

School: .....

Date: .....

On behalf of the Organisation/Local Record Office:

Signed: .....

Name (PRINT): .....

Job Title: .....

Organisation: .....

Date: .....

Please return completed form to the school for permanent retention.

Proforma for individual pupil records to be converted to electronic media

Original Unique Identifier	Full Name of Pupil (SURNAME, Forename(s)	Date of Birth (DD/MM/YYYY)	Original Format of Record	New Format of Record	Date Digitised	New Unique Identifier

On behalf of the school:

Signed: .....

Name (PRINT): .....

Job Title: .....

School: .....

Date: .....

On behalf of the digitising organisation:

Signed: .....

Name (PRINT): .....

Job Title: .....

Organisation: .....

Date: .....

Destruction of original records must be undertaken and recorded in accordance with normal destruction controls and procedures. Destruction of records must be authorised by [insert appropriate person]. Original records must be retained for a period of [insert timeframe of 3 – 6 months] before destruction. Please return completed form to the school for permanent retention.

978-1-9161239-1-5

School Closures and Record Keeping

When a school closes, records management is often low on the list of priorities. However, it is vital to carefully sort and review records in advance of the school closure, to ensure continued compliance with record-keeping obligations.

There are several reasons why a school may close, which may affect where the records need to be stored and managed:

1. Conversion to Academy Status

If a secondary school closes and subsequently becomes an Academy, all records relating to pupils who are transferring to the Academy must be transferred. If the Academy is retaining the existing buildings, then all records relating to the management of the buildings should also be transferred. All other records created and managed when the school was part of the Local Authority (LA) will become the responsibility of the LA.

Please note: A LA may decide that the new Academy is responsible for managing all records of the school prior to it receiving Academy status. Each LA should seek legal advice before making any decision about the management of records relating to schools which have become Academies.

2. Sale or Re-use of the Site

If the school site is being sold or reallocated to another use, then the LA must take responsibility for the records from the date the school closes.

3. Merger of Schools

If two schools are to be merged into one school, the new school is responsible for retaining all current records originating from the former schools.

The school must determine one of four possible outcomes for each group of records:

i. Securely destroy all records which are expired and due for disposal, in accordance with legal and business retention requirements, as detailed on the Retention Schedule.

ii. Transfer to successor school or Academy all records which are current and which will be required by the new school or Academy.

iii. Transfer to the LA all records which are dormant but still need to be retained in order to comply with legal and business retention requirements. This will include records of pupils and employees who are no longer at the school, all administrative and financial records up to the point of closure, etc.

iv. Transfer to the Local Record Office any records with historical value, as detailed on the Retention Schedule, or which are found as part of the sorting exercise, e.g. registers, photographs, log books, etc.

4. Responsibilities

School – Responsible for identifying which records need to be destroyed or transferred to the LA, new school/Academy or Local Record Office. The school must notify the other organisations as soon as possible so that necessary disposal, storage and transfer arrangements can be made. The school must notify their ICT department or supplier to discuss arrangements for the safe transfer or deletion of electronic records, including all back-up copies.

Local Authority – Responsible for the physical transfer, storage and management of all records transferred to their care. Arrangements should be made for the appropriate storage of records, to ensure adequate security and access controls. Consideration should be given to ensure records can be easily identified, in accordance with Data Protection legislation and Freedom of Information and administrative requirements. A system should be in place to identify records when they reach expiry and arrangements should be made to securely and confidentially destroy records. The LA is liable for all transfer, storage and management costs from the time the records are received to the time they are destroyed.

Local Record Office – Responsible for the physical transfer, storage, management and permanent preservation of all records deposited to their care. Records containing personal, sensitive or confidential information must be subject to the applicable closure period. Public access to records must be provided, providing they are not subject to any closure period.

5. Sorting of Records

Sorting of records is time consuming, especially if records management has not been a priority in the past. Sufficient time and resources must be allocated to ensure records are destroyed in accordance with confidentiality and retention requirements, and that records to be transferred to the LA, new school/Academy or Local Record Office have been properly sorted, listed and boxed.

A project to sort records could be managed in the following way:

- Review all records held within the school as soon as notification of closure is received. This must include all records held in all formats, including paper and those created and stored electronically
- Using the Retention Schedule (see Retention Schedule section), categorise records into those to be destroyed, transferred to the new school or Academy, transferred to the LA or transferred to the Local Record Office
- Contact the new school/Academy, LA or Local Record Office to make the necessary arrangements for the safe and secure transfer of records
- Sort, list and box the records in preparation for transfer, ensuring records are stored in a safe environment whilst awaiting collection
- Plan how disposal of records will be undertaken (see Disposal section)
- Sort expired records in readiness for confidential disposal, ensuring they are stored securely whilst awaiting disposal.

6. Security and Confidentiality

Security and confidentiality controls must be maintained throughout the sorting, transfer and disposal exercise. Failure to do so could result in accidental loss, or a data breach under Data Protection legislation, which may result in action from the Information Commissioner's Office.
All filing cabinets, desks, shelves, cupboards and other forms of storage must be completely emptied before the building is vacated or before disposal. This includes removing all drawers from their housing cabinet to ensure nothing has fallen behind.

Records awaiting disposal or transfer to the LA, new school/Academy or Local Record Office must be held in a secure area.

The identity of any third parties collecting or disposing of records must be checked and a collection receipt must be obtained.

Records must not be disposed of in ordinary waste bins or skips. Instead they must be either shredded or put into secure confidential waste sacks (see Disposal section).

Electronic records must be either transferred to the LA, Local Record Office or new school/Academy or deleted in accordance with the organisation's IT Policy.

All IT equipment must be decommissioned in accordance with the organisation's IT Policy (see Disposal section).

Under no circumstances should any records be left behind once the building is vacated.

It is important to bear in mind that when a school closes

978-1-9161239-1-5

the staff teams may feel a real sense of bereavement and this will affect the way in which they view the work which has to be done before the school closes. Sorting out records is usually low on the priority list, but nonetheless needs to be undertaken. Managers will need to consider this when allocating the different elements of the task and when deciding project timescales.

It is advisable to contact the LA, Local Record Office, ICT provider, information governance/records manager and any other third parties, such as confidential waste contractors and removal companies, as soon as possible to ensure timescales and deadlines are realistic, in order to discuss requirements and procedures and to make the necessary arrangements for the safe transfer or disposal of records.

Acknowledgements

Original content by:

John Davies	TFPL Consultancy

Amendments made by the following as part of the 2018 Review:

Andrea Binding	Somerset County Council
Lizi Bird	Solihull Metropolitan Borough Council

Checklist for Storage of Physical Records

Appropriate Storage for Physical Records
Records must be stored in the workplace in a way that does not cause a health and safety hazard. Records must not be stored in corridors or gangways and must not impede or block fire exits. There should be - where appropriate - heat/smoke detectors connected to fire alarms, a sprinkler system and the required number of fire extinguishers. The area in which records are stored should be secured against intruders and have controlled access to the working space.

Storage areas should be regularly monitored and checked for any damage or emerging risks, especially during holiday periods.

Hazards
The following are hazards which need to be considered before approving areas where physical records can be stored:

Environmental Damage - Fire
Records can be damaged beyond repair by fire. Smoke and water damage will also occur to records which have been in a fire, although generally records damaged by smoke or water can be repaired.

Core records should be kept in cabinets or cupboards. Metal filing cabinets will usually suffice, but, for important core records, fireproof cabinets may need to be considered. However, fireproof cabinets are expensive and very heavy, so they should only be used in special circumstances. Core records should be identified so that they may receive priority salvage or protection in the event of an incident affecting the storage area.

Records which are stored on desks, shelves or in cupboards which do not have doors will suffer more damage than those which are stored in cupboards/cabinets which have close-fitting doors.

Environmental Damage – Water
Records damaged by water can usually be repaired by a specialist document salvage company. The salvage process is expensive; therefore, records need to be protected against water damage where possible. Where flooding is involved the water may not always be clean and records could become contaminated as well as damaged.

Records should not be stored directly under water pipes or in places which are liable to flooding (either from excess rainfall or from the overflow of toilet cisterns). Records should be stored in cabinets/cupboards with tight fitting doors which provide protection from water ingress. Records stored on desks or in cabinets/cupboards without close fitting doors will suffer serious water damage.

Records should be stored at least 2 inches off the ground (most office furniture stands at this height). Portable storage containers (i.e. boxes or individual filing drawers) should be raised off the ground by at least 2 inches. This is to ensure that, in the case of a flood, records are protected against immediate flood damage.

Storage areas should be checked for possible damage after extreme weather to ensure no water ingress has occurred.

Environmental Damage – Sunlight
Records should not be stored in direct sunlight (e.g. in front of a window). Direct sunlight will cause records to fade and the direct heat causes paper to dry out and become brittle.

Environmental Damage – High Levels of Humidity
Records should not be stored in areas which are subject to high levels of humidity. Excess moisture in the air can result in mould forming on the records. Mould can be a hazard to human health and will damage records, often beyond repair.

The temperature in record storage areas should not exceed 18oC and the relative humidity should be between 45% and 65%. Temperature and humidity should be regularly monitored and recorded. Storage areas should be checked for damage after extreme weather conditions to reduce the risk of mould growth.

978-1-9161239-1-5

Environmental Damage – Insect/Rodent Infestation

Records should not be stored in areas which are subject to insect infestation or which have a rodent problem (rats or mice). Frequent checks should be made to ensure that infestation has not occurred.

Disaster Recovery Kit

A disaster recovery kit should be at hand, for use in the event of an incident affecting the store. This should include basic equipment, such as mops, buckets and plastic sheeting, for managing a small-scale incident, as well as personal protective equipment such as gloves, hard hats etc.

Cleaning

Physical storage areas should be kept clean and tidy. Rubbish should be removed and chemicals and cleaning materials also removed, or kept in designated storage cabinets so that they do not create a fire hazard.

Electrical Equipment

Use of electrical equipment within physical storage areas should be kept to a minimum in order to reduce fire risks, with all equipment being switched off and unplugged when not in use.

The General Data Protection Regulations (GDPR)

The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). All schools need to comply with this legislation. As part of the Government's initiative, the Department for Education has produced a specific Data Protection Toolkit which can be found at https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

The GDPR Section includes the following sub-sections:

GDPR FAQs
Data Protection: Checklist
Consent to Use Personal Data, including:

- Checklist for consent
- Template Consent Form 01
- Template Consent Form 02

Subject Access Request Procedure
Breach Recording

GDPR FAQs
The following FAQs are produced alongside guidance from the Information Commissioner's Office (ICO).

What information does the GDPR apply to?
The GDPR applies to 'personal data', which means any information relating to an identifiable living person that directly or indirectly identifies them, i.e. you can distinguish them from other individuals. A person's name is the most common way of identifying someone; other obviously personal data include date of birth, e-mail address and photographs of individuals.

Whether any information will identify an individual often depends on the context; a wide range of information can constitute personal data.

More than one piece of data may be necessary to identify an individual; that information may already be held, or may be available elsewhere. This means that less obvious information such as ID numbers (e.g. pupil URN/UPN or National Insurance Number, a car registration, financial details, Internet Protocol (IP) address, location information etc.) can also be considered personal information.
Personal data may also include special categories. These are:

- Race
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where this is used for identification purposes)
- Health data
- Sex life or sexual orientation

Special category data is considered sensitive data, you may only process them in more limited circumstances. Criminal conviction and offences data are treated in much the same way.

Personal data can be found in any format; in manual information such as that held in structured paper files and electronic information (e.g. information stored in network files), in systems and on portable memory devices. Personal data can also be found in audio recordings and video footage, such as CCTV.

The following are instances where data is unlikely to be personal data and the requirements of GDPR are therefore unlikely to apply:

- The data is about a deceased person, although a duty of confidentiality may still exist
- The data has been truly anonymised. Anonymous information has to survive the scrutiny of whoever might have access to the data; it should not be possible for someone to work out who the information relates to. Pseudonymised data is different, it can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data
- The data is about companies or public authorities, however, information about individuals acting as sole traders, employees, partners and company directors - where they are individually identifiable and the information relates to them as an individual - may constitute personal data

978-1-9161239-1-5

- The data references an identifiable individual but does not relate to/concern them or their activities.

What should be included in my privacy notice?
The GDPR sets out the information you should supply and when individuals should be informed.

The information you supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge
- Provided at the point of data collection or as soon afterwards as possible.

See the template privacy notice which is provided in the DfE Toolkit.

Are we a public authority under GDPR?
If you are a public authority as defined under the Freedom of Information Act 2000 or Freedom of Information (Scotland) Act 2002, you will be a public authority for the purposes of the GDPR. State schools and Academies in England and Wales are public authorities. State schools in Scotland are not public authorities in their own right but under the control of the relevant local authority; nevertheless, head teachers and governing boards should familiarise themselves with the guidance below.

Do I need to appoint a data protection officer (DPO)?
Under the GDPR, you must appoint a DPO if you:

- Are a public authority
- Carry out large scale systematic monitoring of individuals (for example, online behaviour tracking), or;
- Carry out large-scale processing of special categories of data or data relating to criminal convictions and offences.

Therefore, schools and Academies should appoint a DPO. Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

You must ensure that any other tasks or duties you assign to your DPO do not result in a conflict of interest with their role as DPO.

Can organisations share a DPO?
If you wish, you may appoint a single DPO to act for a group of schools, taking into account their structure and size.

What are the rules on security under the GDPR?
[see also the Information Security section in this toolkit]

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical (such as encryption and authentication), or organisational (such as training and implementation of policy) measures are used. Effectively this means schools should assess what security measures should be implemented to comply with GDPR.

What is a lawful basis for processing and which should I use?
When processing personal data, you need a fair and lawful reason to do so. There are six available lawful bases for processing under GDPR:

1. The data subject has given clear consent for their personal information to be processed for a specific purpose
2. It is necessary for a contract you have with the data subject
3. It is necessary to comply with the law
4. It is necessary to protect someone's life
5. It is necessary to perform a task in the public interest or for official functions
6. It is necessary for your legitimate interests or the legitimate interests of a third party .

No single basis is 'better' or more important than the others – whichever basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing you won't have a lawful basis.

You must determine your lawful basis before you begin processing, and you should document it. Your privacy notice should include your lawful basis for processing as well as the purposes of the processing. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.

If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).

Special category data require more protection; when using this more sensitive data you must identify one of the six lawful bases above and, in addition, one condition from Article 9 of the GDPR. Depending on the Article 6 and Article 9 lawful basis (used in a few circumstances), you may also need to meet a condition under the DPA 2018; conditions and how they are met are listed under Part 1 and Part 2 of Schedule 1 of the act.

If you are processing criminal conviction data or data about offences, the DPA 2018 requires an additional condition to be met because schools are not considered an 'official authority'. The conditions and how they are met are listed under Part 3 of Schedule 1 of the Act.

If you are unsure about the basis for processing then contact your Data Protection Officer.

The lawful basis for your processing can also affect which rights are available to individuals.

Is parental consent always required when collecting or processing children's personal data?

The GDPR contains new provisions intended to enhance the protection of children's personal data, in particular; privacy notices and parental consent for online services offered to children. Article 8 imposes conditions on children's consent, but it does not require parental consent in every case. Other lawful bases may still be available. Article 8 only applies when the controller is:

- offering Information Society Services (ISS) directly to children and;
- wishes to rely on consent as its basis for processing.

If you do wish to rely upon consent as your lawful basis for processing personal data, whether to use children's data or an adult's:

- The consent should be freely given
- The request for consent, and explanation of what the consent is for, should be concise, easy to understand and distinct from information on other matters
- It should be easy for them to withdraw consent at any time
- The child or adult should be asked to actively opt in, because inactivity or default settings do not constitute consent
- Consent needs to be 'granular'; consent for each and every purpose should be sought.

Further guidance, a checklist and templates for using consent to process personal data can be found later in this section.

What is a data breach?

A data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data, transmitted, stored or otherwise processed". It can be accidental or deliberate.

How will personal data breach reporting work in practice?

Under GDPR the reporting of personal data breaches to the ICO becomes a requirement where it is likely to result in a risk to the rights and freedoms of individuals. There is a requirement to record and possibly report the breach within 72 hours of the data controller becoming aware of the incident and, in some cases, this will also mean that the controller will also have to inform the affected individuals. If you are not the data controller, then the most appropriate action would be to notify the data controller immediately.

978-1-9161239-1-5

Regardless of whether a breach needs to be reported to the ICO or not, breaches or potential breaches should always be recorded, contained as far as possible, mitigating action taken (if possible) and assessments made to inform any necessary changes to working practices. A log of breaches should be maintained and regularly reviewed.

Further information can be found in the DfE toolkit and also under Breach Reporting and Assessment later on in this section.

What is the Data Protection Impact Assessment (DPIA) process?

A DPIA is a tool that organisations should use to achieve good practice when bringing in new or revised processing of personal data, by identifying and minimising risks. It is effectively a risk assessment for the processing of personal information. Carrying out DPIAs is part of the school's accountability obligations under GDPR, and an integral part of the "data protection by default and by design" approach.

Under GDPR a DPIA must be carried out when:

- Using new technologies
- The processing is likely to result in high risk to the rights and freedoms of individuals
- Processing is systematic and extensive, this includes profiling, and decisions that have legal – or similarly significant – effectson individuals
- Processing special categories of data, or personal data in relation to criminal convictions or offences on a large scale
- Undertaking large scale, systematic monitoring of public areas (CCTV).

If a DPIA identifies a high risk that cannot be mitigated, the ICO must be consulted.

Does my organisation need to register under the GDPR?

The ICO provides a self-assessment tool which can be found here:
https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

If you needed to register under the Data Protection Act 2018, then you will need to register (and pay a relevant fee) under the Data Protection (Charges and Information) Regulations 2018.

You will likely be contacted directly by the ICO when your fee is due.

Data Protection: Check List

Action	Potential Documents
☐ We have identified different processes and activities which involve personal and/or special categories of information	☐ Inventory of Processing Activities ☐ Summary record (high level) of the school's processing activities
☐ All levels of staff understand how the school will manage privacy	☐ Data Protection Policy
☐ A Privacy Impact Assessment (PIA) is completed for new processes and projects (manual or electronic)	☐ PIA Form ☐ PIA Procedure/Guidelines for staff ☐ PIA Register (to record either results or reason for not completing a PIA)
☐ Our pupils, parents, visitors plus users of the website understand how the school will process their information	☐ Privacy Notice (aka Fair Processing Notice) in plain language covering all mandatory elements ☐ Fair Processing Statements on forms
☐ All staff understand how the school processes their information	☐ Privacy Notice for staff in plain language covering all mandatory elements ☐ Fair Processing Statements on forms
☐ We have identified the processing for which we currently collect consent and have checked this is free choice	☐ Note: Add to Inventory of Processing Activities
☐ The way consent is collected is appropriate; sought using clear and plain language as well as for each purpose/use of the information. Consent can easily be withdrawn at any time	☐ Parental consent form ☐ Consent Withdrawal Form OR Procedure for this in place ☐ Consent form, other
☐ Relevant staff understand how to process a request to access personal information (SAR) and it is easy for individuals to make a request	☐ SAR Procedure ☐ Request Form – optional, but may make it easier to deal with requests because you will have a clearer picture of what the individual wants ☐ Record of disclosure – retain in case of queries or repeat requests
☐ We have reviewed how information is accessed at school, by whom and have checked this is appropriate	☐ Documentation managing access rights to systems and network drives and consideration of how physical/paper information is stored and accessed

978-1-9161239-1-5

Consent to Use Personal Data Guidance

When processing personal data, organisations need a fair and lawful reason to do so. Most public sector organisations process personal data to meet a legal obligation, but if this is not the case sometimes the consent of an individual has to be relied upon.

What is consent?

Consent is one of six lawful bases to process personal data. 'Consent' under the General Data Protection Regulations (GDPR) has a particular meaning; it should always be freely given, specific, informed and an unambiguous indication of an individual's wishes with regard to the processing of their personal data.

When to use consent

Consent to use an individual's personal data should only be sought if you can offer genuine choice and control over how their data is used. An example of an appropriate time to collect consent in a school or Academy setting is asking for consent to use a photograph in a school newsletter or website, etc.; pupils/parents can refuse consent in this instance without any detriment such as being denied an education or other services.

When not to use consent

If a genuine choice cannot be offered , consent is not appropriate and should not be used. If the personal data would still be used without consent, asking for it is misleading and unfair. This could destroy trust, damage reputation and could lead to enforcement action being taken by the Information Commissioner's Office. Collecting consent would be unfair where there is any element of compulsion or pressure. It should be separate from other terms and conditions and should not be a precondition of service provision. Public authorities, including schools, employers and other organisations in a position of 'power' may find it more difficult to show freely-given consent.

If consent is not appropriate as a basis for processing, another lawful basis for processing must be identified.

How to obtain and record consent

A request for consent, and the explanation of what the consent is to be used for, should be concise, easy to understand and distinct from information on other matters. The following information is the minimum to be provided when seeking consent to use personal data:

- Name of the organisation
- Purpose for each use of the data for which consent is sought
- Type of data that will be used
- Details of the right to withdraw consent at any time and how this can be done
- Details of any third parties who will also use the data and why
- If applicable, the location and possible risks of transfers to countries outside of Europe.

Individuals should be asked to actively opt in - silence, inactivity, pre-ticked boxes or other default settings do not constitute consent.

GDPR also requires 'granular' consent for each and every purpose for which data is to be processed. Individuals should be free to choose which purpose or purposes they accept, rather than having to consent to a bundle of purposes or none at all. Returning to the earlier example on consent to use a photograph in school, displaying a child's photo in the classroom is very different in purpose and use to adding a photo of a child to the school website.

Consent can be collected in a number of ways including the signing of a form with tick boxes, ticking a box when visiting a website, or by any other action which clearly indicates an individual's choice. However it is collected, a clear record which demonstrates consent has been obtained needs to be kept. The burden of proof is on the collecting organisation.

Withdrawal of consent

The GDPR gives a specific right to withdraw consent. Organisations need to tell individuals about their right to withdraw at any time, and make it as easy to withdraw their consent as it was to provide it.

The General Data Protection Regulations (GDPR) Continued

Consent and children

The vulnerability of children is considered in the GDPR. Where Information Society Services(ISS) are offered directly to a child under the age of 13 years old, the processing of their personal data shall only be lawful where the consent of a parent/guardian has been obtained. ISS include online services offered directly to the child for marketing purposes, remuneration or creating child user profiles, for example online businesses and social networking sites.

Is consent that was provided pre-GDPR still valid?

There is no set time limit for the validity of consent. How long it lasts will depend on context, potential risks to the privacy of the individual and how likely it is that circumstances may change.

If consent was provided before GDPR was enacted, it will be important to apply the principles of the checklist below to ensure that it is valid and was documented. Check whether existing consents are appropriate and review the way consent is collected. If existing mechanisms comply with GDPR there is no need to obtain fresh consent.

See below for a consent checklist and a template form.

Checklist for consent

This checklist is adapted from the guidance provided by the Information Commissioner's Office (ICO).

Asking for Consent

- ☐ We have checked that consent is the most appropriate lawful basis for processing
- ☐ We have made the request for consent separate from other matters
- ☐ We ask individuals to positively opt in
- ☐ We don't use pre-ticked boxes or any other type of default consent
- ☐ We use clear, plain language that is easy to understand
- ☐ We tell individuals who we are
- ☐ We specify why we want the data and what we're going to do with it
- ☐ We give the option to consent separately to different purposes and types of processing
- ☐ We name any third-party controllers who will be relying on the consent
- ☐ We tell individuals that they can withdraw their consent
- ☐ We ensure that individuals can refuse to consent without detriment
- ☐ We avoid making consent a precondition of a service
- ☐ If we offer online services directly to children, we only seek consent if we have age verification measures (and parental-consent measures for children under 13 years old) in place.

Recording Consent

- ☐ We keep a record of when and how we got consent from the individual
- ☐ We keep a record of exactly what they were told at the time.

Managing consent

- ☐ We regularly review use of consent
- ☐ We have processes in place to refresh consent at intervals appropriate to the context
- ☐ We have procedures in place to allow consent preferences to be checked and managed
- ☐ We make it easy for individuals to withdraw their consent at any time, and inform them how to do so
- ☐ We act on withdrawals of consent as soon as we can
- ☐ We don't penalise individuals who wish to withdraw consent.

Template Consent Form for Schools 01

Instructions for use: The text below can be transferred onto your school's headed paper. Read through making sure it is relevant to your school and how you will use the photos/videos. Text in [square brackets] is an instruction or needs to be replaced with your school's information. Text in red should only be used if relevant, and can be deleted if it is not relevant or changed to black if it is. This template can also be adapted for other forms used to record consent for pupil's personal data, e.g. creation of profiles on external/online software, if consent is necessary.

978-1-9161239-1-5

[INSERT name of school]
Consent for Children to Appear in Photographs or in Videos and How They Will Be Used

We occasionally take photographs of the children at our school. These images may be used in [INSERT HOW YOU WILL USE, e.g. our school prospectus, in other printed publications that we produce, on our school website, on project display boards in school, etc.]. We may also make video or webcam recordings for **[INSERT HOW YOU WILL USE, e.g. school-to-school conferences, examinations and coursework].**

It is important that we protect your child's interests, respect your wishes and comply with Data Protection law. Please read the Conditions of Use below before answering the questions below and signing and dating this form. Please return the completed form (one for each child) to the school as soon as possible; we will not use a photograph or video of your child without consent.

Please note there are certain activities where we do not use consent as the basis for processing your child's data. There are described in our Privacy Notices **[INSERT WHERE AVAILABLE, e.g. website link]**. We may also take photos/video of your child for identification purposes and for evidencing their educational development – such data will sit on their file and not be shared unless the law requires us to do so or you have given your specific consent.

Where your child is over 13 years of age, we recommend that you complete this form with them, as children may be able to decide how their data may be used in certain circumstances.

Please note that you can withdraw your consent at any time. If you have any queries or wish to withdraw or review your consent, you can contact **[INSERT School Lead/Data Protection Officer]**

Conditions of Use:

- This form is valid [INSERT TIME VALID FOR e.g. for the period of one school year]. Your consent will automatically expire after this time
- The school will not re-use any photographs or recordings of your child that are incompatible with the original purposes explained to you
- If we use photographs of individual pupils, we will not use the full name of that child in any accompanying text or caption without consent, nor will we include any other personal data
- We may use group or class photographs or footage with very general labels, such as 'a science lesson'
- We will only use photographs and videos of pupils who are suitably dressed
- Parents should note that websites can be viewed throughout the world and not just in the United Kingdom (where UK law applies) and, when copied from the website, images and information can no longer be controlled by the school.
- [INSERT ANY FURTHER AND RELEVANT CONDITIONS]

Further information on how we use your data and your child's personal data is in the Privacy Notice(s) available **[INSERT WHERE AVAILABLE, e.g. website link].**

The General Data Protection Regulations (GDPR) Continued

Description of the use of Photographs or Images	Please tick	
May we use your child's photograph and first name on display boards within the school building? Please note: Displays are generally viewed by staff, pupils, parents, guardians and other visitors to the school	Yes ☐	No ☐
May we use your child's photograph in the school hard-copy prospectus and other printed publications that we produce for promotional purposes? Please note: Printed publications are available to anyone	Yes ☐	No ☐
May we put your child's photograph and/or name on the school's website, including in on-line publications such as an on-line prospectus and other promotional material? Please note: Websites can be viewed throughout the world, not just the United Kingdom where UK law applies and, if copied from the website, images and information can no longer be controlled by the school	Yes ☐	No ☐
May we use your child's photograph and name on Social Media [specify type]? Please note: Social Media can be viewed throughout the world, not just the United Kingdom where UK law applies and if copied from Social Media, images and information can no longer be controlled by the school	Yes ☐	No ☐
May we record your child on video for [INSERT WHEN YOU MAY DO THIS, e.g. Nativity play, internal school events, external school events and trips]. Please note: this may include your child's voice as well as their image. Videos will only be made available to parents/guardians of the child	Yes ☐	No ☐
[INSERT ANY OTHER USES OF PHOTOGRAPHS/VIDEOS YOU WISH TO GAIN CONSENT FOR]	Yes ☐	No ☐

Name of Child: ----------

Name of Parent/Carer: ----------

Signed:

(Parent/Carer) ----------

Date: ----------

978-1-9161239-1-5

Template Consent Form for Schools 02

Instructions for use: The text below can be transferred onto your schools headed paper. Read through making sure it is relevant to your school and the event being held. Text in [square brackets] is an instruction or needs to be replaced with your school's information. Text in red should only be used if relevant and can be deleted if it is not or changed to black if it is. This template can also be adapted for other consent forms to use pupil's personal data, e.g. creation of profiles on external/online software, if consent is necessary.

[INSERT name of school]
Specific Consent for Children to Appear in Photographs or in Videos

Occasionally, our school is visited by the media who will take photographs or film footage of a high-profile event, or to celebrate a particular achievement. Pupils will often appear in these images, which may appear in local or national newspapers or on televised news programmes. One such event is due to take place and I am writing to inform you of this and ask permission for your child's involvement.

It is important that we protect your child's interests, respect your wishes and comply with Data Protection law. Please read the Conditions of Use below before completing and signing and dating the form below. Please return the completed form (one for each child) to the school as soon as possible; we will not allow your child to be involved with the media coverage without your consent.

Where your child is over 13 years of age, we recommend that you complete this form eith them, as children may be able to decide how their data may be used in certain circumstances.

Please note that you can withdraw your consent at any time. If you have any queries or wish to withdraw or review your consent, you can contact **[INSERT School Lead/Data Protection Officer]**

Conditions of Use:

- This form is valid [INSERT TIME VALID FOR e.g. for the duration of the event]. Your consent will automatically expire after this time
- The school will not re-use any photographs or recordings of your child that are incompatible with the original purposes explained to you
- We may use group or class photographs or footage with very general labels, such as 'a science lesson'
- We will only use photographs and videos of pupils who are suitably dressed
- Parents should note that websites can be viewed throughout the world and not just in the United Kingdom (where UK law applies) and, if copied from the website, images and information can no longer be controlled by the school.
- [INSERT ANY FURTHER AND RELEVANT CONDITIONS]

Please note: If you give permission for your child's image to be used by the media then you should be aware that:

- The media will want to use any printed or broadcast media pictures that they take alongside the relevant story
- It is likely that they will wish to publish the child's name, age and the school name in the caption for the picture (possible exceptions to this are large group or team photographs)
- It is possible that the newspaper will re-publish the story on their website, or distribute it more widely to other newspapers.

Further information on how we use your data and your child's personal data is in Privacy Notice(s) available [INSERT WHERE AVAILABLE, e.g. website link].

The General Data Protection Regulations (GDPR) Continued

Description of event: [INSERT description here]
Purposes for which the [DELETE AS APPROPRIATE photograph/video/child's name] will be used: [INSERT purpose here]
Description of coverage: [INSERT names of newspapers/TV channels and any other relevant details]

May we allow your child to appear in the media coverage as described above? Please note: once a photograph appears in the media the school has no control over who else may use the images/storyline	Yes ☐	No ☐

I have read and understand the conditions of use attached to this form.

Name of Child ----------

Name of Parent/Carer ----------

Signed ----------

(Parent/Carer) ----------

Dated ----------

978-1-9161239-1-5

Subject Access Request Procedure

This is a suggested procedure for schools to follow, in order to help them process a Subject Access Request (SAR) appropriately and within the required timescales. A template SAR form has also been provided for schools to adapt should they wish, but they are not mandatory.

Receiving a SAR

A Subject Access Request (SAR) is received from a pupil, parent, member of staff or other individual for whom the school holds information. This may be received either verbally, in writing or via a form (see example template below) which is made available on the website or from the school office.

Pass the SAR to the Data Protection Officer or person responsible for processing SARs, who will acknowledge receipt of the request.

If the request is in writing or via a form ensure it is clear what the individual wants. If the request is received verbally it may be appropriate to seek clarification from the requestor to ensure the correct information is sought for them. Seek confirmation of the information the individual would like if it is not clear.

Check identity and authorisation

Ask the requestor to provide evidence of their identity in the form of a current passport/driving license. This may not be necessary if the requestor is known and you are sure they are who they say they are. Keep a record of the identification checks that were conducted.

If the requestor is making a SAR on behalf of a pupil or other individual, ensure that they have the authority to do so; for example, a request can be made by a solicitor or by a parent on behalf of their child where they have parental responsibility or they have care of the child, however, individual circumstances should be considered.

If the child is deemed to be competent to make their own request (usually only relevant in secondary settings) then the information should be released to them or their consent sought.

Collect and prepare the data

Collect the data requested. This may require searching across multiple filing systems, formats and systems/databases in the school, as well as archived files, e-mail folders and archives.

Don't provide original documents to the requestor: instead make copies of documents, or copy and extract the relevant data.

Review the data to identify whether any third-party data are present in it, and either redact the identifying third party information from the documentation – this may not just be limited to a name, other information may identify them - or obtain written consent from the third party for their identity and personal data to be revealed. In practice, staff names will generally remain (where acting in their professional capacity) but the data and names of pupils and parents will need to be redacted.

Supply the data

Consider how you will supply the requestor with the data and whether any security precautions should be taken (such as confirming the address, sending special delivery or handing directly to them).

Meet the legal requirement to provide the requested data to the requestor within one calendar month from the date on which the request was received. A further 2 months can be taken to respond if the request is of a particularly complex nature, however, the requestor should be made aware of this as soon as possible.

Keep a record

On a SAR log maintain a record of requests for data, receipt of the data, and relevant dates.

It is useful to retain a copy, for a short period, of the data provided, as well as any information withheld. This is so that queries or a request for a review can be responded to.

Template SAR Form

School Data Subject Access Request Form

If you wish to make a request for personal data under Data Protection legislation please complete the form below to enable us to meet your request. The form is not mandatory; however, it will help us to respond to your request as quickly as possible. The school will endeavour to respond to your request within one calendar month. We may extend this time if the request is complex, however we will inform you of this within one month of receipt of the request, together with the reason(s) for delay.

The form can be submitted to the school via e-mail to **[INSERT contact e-mail] or by posting to [INSERT contact and address].**

Your name:		**E-mail or postal address: (whichever is your preferred contact method)**		
Phone number: (optional - used to contact you about request)				
Are you the Data Subject?	Yes ☐	No ☐	**If you selected 'No', add name of Data subject:**	
Your relationship to the Data Subject, or state 'Not applicable':				
If you are requesting data on behalf of a child, please note that we may consult with the child if we believe that they have the capacity to understand this request.				
Do you want a copy of some personal data?	Yes ☐	No ☐	**If No**, please select another option below:	
Information about processing ☐	Correction of data ☐	Erasure of data ☐	Objection to/Restrict use of data ☐	
If Yes, what data? Please describe below and provide as much detail as possible to aid us in our search				
Have you enclosed/attached a copy of your photo ID?	Yes ☐	No ☐		
Please sign:		**Date:**		

978-1-9161239-1-5

Breach Recording

[For additional information about breach recording see also under the Information Security section of this toolkit]

A personal data breach is defined as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Under the GDPR, breaches which are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the Information Commissioner's Office (ICO). Where reporting is required, it should be done within 72 hours of discovery.

Regardless of whether a breach needs to be reported to the ICO, breaches or potential breaches should always be recorded, mitigating action taken (if possible), and assessed to inform whether or not any changes to working practices are required. In making the assessment, the school should consider the likely impact on data subjects including:

- Physical threat to safety
- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned.

When the personal data breach is likely to result in a high risk to the rights and freedoms of affected individuals, it may be appropriate to inform those impacted by the personal data breach. Informing people and organisations that have experienced an incident can be an important element in helping to manage the situation; for example, notifying an individual whose information was misdirected would help them take to precautions against ID theft, fraud etc. However, if notification would serve only to worry the person concerned without any benefit, it may not be appropriate. Notification should have a clear purpose.

The purpose of the Breach Recording and Assessment form is to:

- Provide a consistent approach to responding to information security breaches
- Determine whether the ICO should be notified about the incident
- Provide an overview of the incident for the Head Teacher/ Chair of Governors along with recommendations on what action should be taken to address matters and to prevent a reoccurrence.

Further information can be found in the DfE toolkit.

The assessment form will support a school in considering:

- Containment
- Level of risk
- Notification
- Evaluation and response.

Template Breach Recording Form

[INSERT name of school]
Record of Data Protection Breach

Name of Data Protection Officer:
ICO registration number:

Completed by (Name):	
Job title:	
Contact e-mail address and phone number:	
Date breach occurred:	
Date breach discovered:	
Date breach reported:	
Date investigation started:	
Date investigation completed:	
Description and nature of the breach:	
Number of Data Subjects involved:	
Volume of personal data:	
Category of personal data: *List the broad types of information*	
Further details of the personal data:	
Containment Action: *Summarise actions taken to recover from the mistake, measures taken to mitigate any possible adverse effects on the individual(s) concerned and actions taken to stop it getting worse, e.g. 'collected information', or 'asked recipient to delete it'.*	
Risks as a result of the breach: *Describe the risks or consequences; for example, if the information contained financial data such as bank account numbers, then there may be a risk of fraud, or if the information contained sensitive health and personal data then there may be a safeguarding issue that could leave the affected individual vulnerable.*	

978-1-9161239-1-5

Overall impact of the breach: *Consider: Sensitivity of the data; volume of data; and; potential detriment to individuals.*	
Impact of the breach on Data Subject:	
Assess who should be notified: *List and state why - informing people and organisations that have experienced an incident can be an important element in helping to manage the situation. Notifying a person whose information got misdirected, for example, would help them to take precautions against ID theft, fraud etc. Also consider if notification would serve only to worry them without any benefit; informing people about an incident is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.*	
Notification recommendation: *Tick all those that apply, adding additional information if required. Keep a record of the notification.*	
Evaluation: *Summarise the lessons learnt.* *Measures to be taken by the school to reduce the likelihood of such incidents from happening again:* *Consider adding to an action plan, with time for a review to check if measures have been implemented.*	
Senior staff sign off and recommendations:	The Head Teacher/Chair of Governors/DPO have read and reviewed the form and discussed the matters with relevant members of staff to reach the below conclusions: Agree/Do not agree [delete as applicable] with the assessment of risk and recommendations' The breach is not/is [delete as applicable] deemed reportable to the Information Commissioner. [Add additional points as required]
Signature:	
Name:	
Job title:	

Acknowledgements:

Andy Crow	Chorus Business Advisers Ltd
Thomas Ng	West Berkshire Council
Lizi Bird	Solihull Metropolitan Borough Council

Retention Guidelines

Introduction

1. The purpose of the retention guidelines

Under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) schools need a policy setting out retention periods for the personal data they hold. Also, under the Freedom of Information Act 2000, schools should maintain a Retention Schedule listing the series of records which the school creates or maintains in the course of its business.

The Retention Schedule lays down the length of time for which the record needs to be retained and the action which should be taken when it is of no further administrative or legal use. It also lays down the basis for normal processing under both Data Protection and Freedom of Information legislation.

Members of staff are expected to manage their current record keeping systems using the Retention Schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The Retention Schedule refers to series' of records regardless of the media (e.g. paper/electronic/microfilm/photographic etc.) in/on which they are stored.

2. Benefits of a Retention Schedule

There are a number of benefits which arise from the use of a complete Retention Schedule:

- Managing records against the Retention Schedule is deemed to be 'normal processing' under the Data Protection legislation and the Freedom of Information Act
- Members of staff can be confident about the safe disposal of information at the appropriate time
- Information which is subject to Freedom of Information and Data Protection legislation will be available when required
- The school is not maintaining and storing information unnecessarily.

Members of staff should be aware that once a Freedom of Information request is received, or a legal hold imposed, then records disposal relating to the request or legal hold must be stopped.

Records which may be required by IICSA should be treated as though they are subject to a legal hold.

3. Maintaining and amending the Retention Schedule

Where appropriate the Retention Schedule should be reviewed and amended to include any new record series created, and any obsolete record series removed.

This IRMS Retention Schedule contains recommended retention periods for the different record series created and maintained by schools in the course of their business. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute, others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of Data Protection and Freedom of Information legislation.

If record series are to be kept for longer or shorter periods than laid out in this document then the reason(s) for this need to be documented.

This schedule should be reviewed on a regular basis.

Where there is a recommendation to archive the information this may be in an electronic format. There is no need to convert the information into a hard copy. Such records should be kept in separate electronic folder suitably marked as holding archival material.

Disclaimer

This document is a guideline only and liability is the responsibility of the end user and not of the IRMS. Individual organisations should seek the appropriate legal advice and senior management approval.

These retention guidelines are free for use to schools. Questions will only be dealt with if they are submitted by IRMS members. Please complete the form on the webpage, remembering to include your IRMS membership number.

978-1-9161239-1-5

Further details about the benefits of IRMS membership can be found at: http://www.irms.org.uk/join

4. Using the Retention Schedule

The Retention Schedule is divided into 5 sections:

1 Governing Body
- 1.1 Management of Governing Body
- 1.2 Governor Management

2 School Management
- 2.1 Head Teacher and Senior Management Team
- 2.2 Operational Administration
- 2.3 Human Resources
- 2.4 Health and Safety
- 2.5 Financial Management
- 2.6 Property Management

3 Pupil Management
- 3.1 Admissions Process
- 3.2 Pupil's Educational Record
- 3.3 Attendance
- 3.4 Special Educational Needs

4 Curriculum and Extra-Curricular Activities
- 4.1 Statistics and Management Information
- 4.2 Implementation of Curriculum
- 4.3 School Trips
- 4.4 School Support Organisations

5 Central Government and Local Authority
- 5.1 Local Authority
- 5.2 Central Government

There are sub headings under each section to help guide you to whichever retention period you are looking for. Each entry has a unique reference number. If you are sending a query to the IRMS about an individual retention period, please ensure that you have quoted the unique reference number.

Acknowledgements

Keith Batchelor	Batchelor Associates
Elizabeth Barber	Kent County Council
Molly Kirkham	Gloucestershire County Council
Catrina Finch	City of Wolverhampton Council

Retention Guidelines

1 Governing Body

This section contains retention periods connected to the work and responsibilities of the governing body.

For further information about governing body records please see: "The constitution of governing bodies of maintained schools Statutory guidance for governing bodies of maintained schools and local authorities in England August 2017"

1.1 Management of Governing Body					
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
1.1.1	Instruments of government		For the life of the school	Consult local archives before disposal	
1.1.2	Trusts and endowments		For the life of the school	Consult local archives before disposal	
1.1.3	Records relating to the election of parent and staff governors not appointed by the governors		Date of election + 6 months	SECURE DISPOSAL	Yes
1.1.4	Records relating to the appointment of co-opted governors		Provided that the decision has been recorded in the minutes, the records relating to the appointment can be destroyed once the co-opted governor has finished their term of office (except where there have been allegations concerning children). In this case retain for 25 years	SECURE DISPOSAL	Yes

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
1.1.5	Records relating to the election of chair and vice chair		Once the decision has been recorded in the minutes, the records relating to the election can be destroyed	SECURE DISPOSAL	Yes
1.1.6	Scheme of delegation and terms of reference for committees		Until superseded or whilst relevant [Schools may wish to retain these records for reference purposes in case decisions need to be justified]	These could be offered to the archives if appropriate	
1.1.7	Meetings schedule		Current year	STANDARD DISPOSAL	
1.1.8	Agendas - principal copy		Where possible the agenda should be stored with the principal set of the minutes	Consult local archives before disposal	Potential
1.1.9	Minutes - principal set (signed)		Although generally kept for the life of the organisation, the Local Authority is only required to make these available for 10 years from the date of the meeting	Consult local archives before disposal	Potential

Retention Guidelines Continued

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
1.1.10	Reports made to the governors' meeting which are referred to in the minutes		Although generally kept for the life of the organisation, the Local Authority is only required to make these available for 10 years from the date of the meeting	Consult local archives before disposal	Potential
1.1.11	Register of attendance at Full governing board meetings		Date of last meeting in the book + 6 years	SECURE DISPOSAL	Yes
1.1.12	Papers relating to the management of the annual parents' meeting		Date of meeting + 6 years	SECURE DISPOSAL	Yes
1.1.13	Agendas - additional copies		Date of meeting	STANDARD DISPOSAL	
1.1.14	Records relating to Governor Monitoring Visits		Date of the visit + 3 years	SECURE DISPOSAL	Yes
1.1.15	Annual Reports required by the DoE		Date of report + 10 years	SECURE DISPOSAL	
1.1.16	All records relating to the conversion of schools to Academy status		For the life of the organisation	Consult local archives before disposal	

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
1.1.17	Records relating to complaints made to and investigated by the governing body or head teacher		Major complaints: current year + 6 years. If negligence involved then: current year + 15 years If child protection or safeguarding issues are involved then: current year + 40 years	SECURE DISPOSAL	Yes
1.1.18	Correspondence sent and received by the governing body or head teacher		General correspondence should be retained for current year + 3 years	SECURE DISPOSAL	Potential
1.1.19	Action plans created and administered by the governing body		Until superseded or whilst relevant	SECURE DISPOSAL	
1.1.20	Policy documents created and administered by the governing body		Until superseded [The school should consider keeping all policies relating to safeguarding, child protection or other pupil related issues such as exclusion until the IICSA has issued its recommendations.]		

1.2	Governor Management				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
1.2.1	Records relating to the appointment of a clerk to the governing body		Date on which clerk appointment ceases + 6 years	SECURE DISPOSAL	Yes
1.2.2	Records relating to the terms of office of serving governors, including evidence of appointment		Date appointment ceases + 6 years		Yes
1.2.3	Records relating to governor declaration against disqualification criteria		Date appointment ceases + 6 years	SECURE DISPOSAL	Yes
1.2.4	Register of business interests		Date appointment ceases + 6 years	SECURE DISPOSAL	Yes
1.2.5	Governors Code of Conduct		This is expected to be a dynamic document; one copy of each version should be kept for the life of the organisation		
1.2.6	Records relating to the training required and received by Governors		Date Governor steps down + 6 years	SECURE DISPOSAL	Yes

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
1.2.7	Records relating to the induction programme for new governors		Date appointment ceases + 6 years	SECURE DISPOSAL	Yes
1.2.8	Records relating to DBS checks carried out on clerk and members of the governing body		Date of DBS check + 6 months	SECURE DISPOSAL	Yes
1.2.9	Governor personnel files		Date appointment ceases + 6 years	SECURE DISPOSAL	Yes

2 Management of the School

This section contains retention periods connected to the processes involved in managing the school, including Human Resources, Financial Management, Payroll and Property Management.

2.1	Head Teacher and Senior Management Team				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
2.1.1	Log books of activity in the school maintained by the Head Teacher		Date of last entry in the book + minimum of 6 years, then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate	Potential
2.1.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies		Date of the meeting + 3 years then review annually, or as required if not destroyed	SECURE DISPOSAL	Potential
2.1.3	Reports created by the Head Teacher or the Management Team		Date of the report + a minimum of 3 years then review annually or as required if not destroyed	SECURE DISPOSAL	Potential

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
2.1.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities which do not fall under any other category		Current academic year + 6 years then review annually, or as required if not destroyed	SECURE DISPOSAL	Potential
2.1.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities		Current year + 3 years	SECURE DISPOSAL	Potential
2.1.6	Professional development plans		These should be held on the individual's personnel record. If not then termination of employment + 6 years	SECURE DISPOSAL	Potential
2.1.7	School development plans		Life of the plan + 3 years	SECURE DISPOSAL	

978-1-9161239-1-5

2.2	Operational Administration				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
2.2.1	General file series which do not fit under any other category		Current year + 5 years, then review	SECURE DISPOSAL	Potential
2.2.2	Records relating to the creation and publication of the school brochure or prospectus		Current academic year + 3 years	The school could preserve a copy for their archive otherwise STANDARD DISPOSAL	
2.2.3	Records relating to the creation and distribution of circulars to staff, parents or pupils		Current academic year + 1 year	STANDARD DISPOSAL	
2.2.4	School Privacy Notice which is sent to parents as part of GDPR compliance		Until superseded + 6 years		
2.2.5	Consents relating to school activities as part of GDPR compliance (for example, consent to be sent circulars or mailings)		Consent will last whilst the pupil attends the school, it can therefore be destroyed when the pupil leaves	SECURE DISPOSAL	Yes
2.2.6	Newsletters and other items with a short operational use		Current academic year + 1 year [Schools may decide to archive one copy]	STANDARD DISPOSAL	
2.2.7	Visitor management systems (including electronic systems, visitors books and signing-in sheets)		Last entry in the visitors book + 6 years (in case of claims by parents or pupils about various actions).	SECURE DISPOSAL	Yes
2.2.8	Walking bus registers		Date of register + 6 years	SECURE DISPOSAL	Yes

2.3 Human Resources					
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
Recruitment					
2.3.1	All records leading up to the appointment of a headteacher		Unsuccessful attempts. Date of appointment plus 6 months. Add to personnel file and retain until end of appointment + 6 years, except in cases of negligence or claims of child abuse then at least 15 years	SECURE DISPOSAL	Yes
2.3.2	All records leading up to the appointment of a member of staff/governor – unsuccessful candidates		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL	Yes
2.3.3	Pre-employment vetting information – DBS Checks – successful candidates	DBS Update Service Employer Guide June 2014; Keeping Children Safe in Education.2018 (Statutory Guidance from DoE) Sections 73, 74	Application forms, references and other documents – for the duration of the employee's employment + 6 years	SECURE DISPOSAL	Yes

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
Recruitment					
2.3.4	Forms of proof of identity collected as part of the process of checking "portable" enhanced DBS disclosure		Where possible this process should be carried out using the on-line system. If it is necessary to take a copy of documentation then it should be retained on the staff personal file.	SECURE DISPOSAL	Yes
2.3.5	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom – successful candidates	An Employer's Guide to Right to Work Checks [Home Office, May 2015]	Where possible these documents should be added to the staff personnel file [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of employment + not less than 2 years	SECURE DISPOSAL	Yes
Operational Staff Management					
2.3.6	Staff personnel file	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years, unless the member of staff is part of any case which falls under the terms of reference of IICSA. If this is the case then the file will need to be retained until IICSA enquiries are complete	SECURE DISPOSAL	Yes
2.3.7	Annual appraisal/assessment records		Current year + 6 years	SECURE DISPOSAL	Yes

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
Operational Staff Management					
2.3.8	Sickness absence monitoring		Sickness records are categorised as sensitive data. There is a legal obligation under statutory sickness pay to keep records for sickness monitoring. Sickness records should be kept separate from accident records. It could be argued that where sickness pay is not paid then current year + 3 years is acceptable, whilst if sickness pay is made then it becomes a financial record and current year + 6 years applies. The actual retention may depend on the internal auditors. Most seem to accept current year + 3 years as being acceptable as this gives them, 'benefits' and Inland Revenue have time to investigate if they need to	SECURE DISPOSAL	Yes
2.3.9	Staff training – where the training leads to continuing professional development		Length of time required by the professional body	SECURE DISPOSAL	Yes
2.3.10	Staff training – except where dealing with children, e.g. first aid or health and safety		This should be retained on the personnel file [see 2.3.1 above]	SECURE DISPOSAL	Yes

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
Operational Staff Management					
2.3.11	Staff training – where the training relates to children (e.g. safeguarding or other child related training)		Date of the training + 40 years [This retention period reflects that the IICSA may wish to see training records as part of an investigation]	SECURE DISPOSAL	Yes
Disciplinary and Grievance Processes					
Where schools are in any doubt as to which categories disciplinary records fall under, then HR or legal advice should be sought from the Local Authority.					
2.3.12	Records relating to any allegation of a child protection nature against a member of staff	"Keeping children safe in education Statutory guidance for schools and colleges September 2018"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018"	Until the person's normal retirement age or 10 years from the date of the allegation (whichever is the longer) then REVIEW. Note: allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned UNLESS the member of staff is part of any case which falls under the terms of reference of IICSA. If this is the case then the file will need to be retained until IICSA enquiries are complete	SECURE DISPOSAL These records must be shredded	Yes
2.3.13	Disciplinary proceedings				Yes

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
Disciplinary and Grievance Processes					
Note: The ACAS code of practice on disciplinary and grievance procedures recommends that the employee should be told how long a disciplinary warning will remain current. However, this does not mean that the data itself should be destroyed at the end of the set period. Any disciplinary proceedings data will be a record of an important event in the course of the employer's relationship with the employee. Should the same employee be accused of similar misconduct five years down the line, and them defend him- or herself by saying "I would never do something like that", reference to the earlier proceedings may show that the comment should not be given credence. Alternatively, if the employee were to be dismissed for some later offence and then claim at tribunal that he or she had "fifteen years of unblemished service", the record of the disciplinary proceedings would be effective evidence to counter this claim. Employers should, therefore, be careful not to confuse the expiry of a warning for disciplinary purposes with a requirement to destroy all reference to its existence in the personnel file. One danger is that the disciplinary procedure itself often gives the impression that, at the end of the effective period for the warning, the warning will be "removed from the file". This or similar wording should be changed to make it clear that, while the warning will not remain active in relation to future disciplinary matters, a record of what has occurred will be kept.					
	Oral warning		Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file	
	Written warning – level 1		Date of warning + 6 months		
	Written warning – level 2		Date of warning + 12 months		
	Final warning		Date of warning + 18 months		
	Case not found		If the incident is related to child protection then see above, otherwise dispose of at the conclusion of the case	SECURE DISPOSAL	

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
Payroll and Pensions					
2.3.14	Absence record		Current year + 3 years	SECURE DISPOSAL	Yes
2.3.15	Batches	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.16	Bonus sheets	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 3 years	SECURE DISPOSAL	Yes
2.3.17	Car allowance claims	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 3 years	SECURE DISPOSAL	Yes
2.3.18	Car loans	Taxes Management Act 1970 Income and Corporation Taxes 1988	Completion of loan + 6 years	SECURE DISPOSAL	Yes
2.3.19	Car mileage output	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.20	Elements		Current year + 2 years	SECURE DISPOSAL	Yes
2.3.21	Income tax form P60		Current year + 6 years	SECURE DISPOSAL	Yes

Retention Guidelines Continued

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
Payroll and Pensions					
2.3.22	Insurance	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.23	Maternity payment		Current year + 3 years	SECURE DISPOSAL	Yes
2.3.24	Members allowance register	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.25	National Insurance – schedule of payments	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.26	Overtime	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 3 years	SECURE DISPOSAL	Yes
2.3.27	Part time fee claims	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.28	Pay packet receipt by employee		Current year + 2 years	SECURE DISPOSAL	Yes
2.3.29	Payroll awards		Current year + 6 years	SECURE DISPOSAL	Yes

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
Payroll and Pensions					
2.3.30	Payroll – gross/net weekly or monthly	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.31	Payroll reports	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.32	Payslips – copies	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.33	Pension payroll	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.34	Personal bank details	If employment ceases then end of employment + 6 years	Until superseded + 3 years	SECURE DISPOSAL	Yes
2.3.35	Sickness records		Current year + 3 years	SECURE DISPOSAL	Yes
2.3.36	Staff returns		Current year + 3 years	SECURE DISPOSAL	Yes
2.3.37	Superannuation adjustments	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL	Yes

Retention Guidelines Continued

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
Payroll and Pensions					
	Superannuation reports	Taxes Management Act 1970 Income and Corporation Taxes1988	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.38	Tax forms P6/P11/ P11D/P35/P45/P46/ P48	The minimum requirement - as stated in Inland Revenue Booklet 490 - is for at least 3 years after the end of the tax year to which they apply. Originals must be retained in paper/ electronic format. It is a corporate decision to retain for current year + 6 years. Employees should retain records for 22 months after current tax year	Current year + 6 years	SECURE DISPOSAL	Yes
2.3.39	Time sheets/clock cards/flexitime		Current year + 3 years	SECURE DISPOSAL	Yes

978-1-9161239-1-5

2.4	Health and Safety				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
2.4.1	Health and safety policy statements		Life of policy + 3 years	SECURE DISPOSAL	
2.4.2	Health and safety risk assessments		Life of risk assessment + 3 years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred	SECURE DISPOSAL	
2.4.3	Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 Social Security (Claims and Payments) Regulations 1979. SI 1979 No 628 Social Security (Claims and Payments) Regulations SI 1987 No 1968 Revokes all but Part 1 of SI 1979 No 628 Social Security Administration Act 1992 Section 8. Social Security (Claims and Payments) Amendment (No 30 Regulations 1993 SI 1993 No 2113 Allows the information to be kept electronically	The Accident Book – BI 510 - 3 years after last entry in the book This includes the new format to be used from 1/1/04 This means that, if it takes 5 years to complete, the book must be retained for a further 3 years from the last entry Completed pages must be kept secure with restricted access. Data Protection Act 2018 and GDPR	SECURE DISPOSAL	Yes

2.4	Health and Safety				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
2.4.4	Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 Social Security (Claims and Payments) Regulations 1979. SI 1979 No 628 Social Security (Claims and Payments) Regulations SI 1987 No 1968 Revokes all but Part 1 of SI 1979 No 628 Social Security Administration Act 1992 Section 8. Social Security (Claims and Payments) Amendment (No 30 Regulations 1993 SI 1993 No 2113 Allows the information to be kept electronically	The Accident Book – BI 510 - 3 years after last entry in the book This includes the new format to be used from 1/1/04 This means that, if it takes 5 years to complete, the book must be retained for a further 3 years from the last entry Completed pages must be kept secure with restricted access. Data Protection Act 2018 and GDPR	SECURE DISPOSAL	Yes
2.4.5	Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR). For more information see http://www.hse.gov.uk/RIDDOR/	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 SI 2013 No 1471 Regulation 12(2)	Date of incident + 3 years provided that all records relating to the incident are held on personnel file [see 2.4.2 above]	SECURE DISPOSAL	Yes

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
2.4.6	Control of Substances Hazardous to Health (COSHH)	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Date of incident + 40 years	SECURE DISPOSAL	
2.4.7	Process of monitoring of areas where employees and persons are likely to have come into contact with asbestos	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL	
2.4.8	Process of monitoring of areas where employees and persons are likely to have come into contact with radiation. Maintenance records or controls, safety features and PPE ---------- Dose assessment and recording	The Ionising Radiation Regulations 2017. SI 2017 No 1075 Regulation 11 As amended by SI 2018 No 390 Personal Protective Equipment (Enforcement) Regulations 2018	2 years from the date on which the examination was made and that the record includes the condition of the equipment at the time of the examination. ---------- To keep the records made and maintained (or a copy of these records) until the person to whom the record relates has or would have attained the age of 75 years, but in any event for at least 30 years from when the record was made	SECURE DISPOSAL	
2.4.9	Fire Precautions log books		Current year + 3 years	SECURE DISPOSAL	

2.4	Health and Safety				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
2.4.10	Health and safety file to show current state of building, including all alterations (wiring, plumbing, building works, etc.), to be passed on in the case of change of ownership		Pass to new owner on sale or transfer of building		
2.5	**Financial Management**				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
Risk Management and Insurance					
2.5.1	Employer's Liability Insurance Certificate		Closure of the school + 40 years [May be kept electronically]	SECURE DISPOSAL To be passed to the Local Authority if the school closes	
Asset Management					
2.5.2	Inventories of furniture and equipment		Current year + 6 years	SECURE DISPOSAL	
2.5.3	Burglary, theft and vandalism report forms		Current year + 6 years	SECURE DISPOSAL	
Accounts and Statements (including budget management)					
2.5.4	Annual accounts		Current year + 6 years	STANDARD DISPOSAL	
2.5.5	Loans and grants managed by the school		Date of last payment on the loan + 12 years then review	SECURE DISPOSAL	

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
Accounts and Statements (including budget management)					
2.5.6	All records relating to the creation and management of budgets, including the annual budget statement and back-ground papers		Life of the budget + 3 years	SECURE DISPOSAL	
2.5.7	Invoices, receipts, order books and requisitions, delivery notices		Current financial year + 6 years	SECURE DISPOSAL	
2.5.8	Records relating to the collection and banking of monies		Current financial year + 6 years	SECURE DISPOSAL	
2.5.9	Records relating to the identification and collection of debt		Final payment of debt + 6 years	SECURE DISPOSAL	
Pupil Finance					
2.5.10	Student Grant applications		Current year + 3 years	SECURE DISPOSAL	Yes
2.5.11	Pupil Premium Fund records		Date pupil leaves the provision + 6 years	SECURE DISPOSAL	Yes
Contract Management					
2.5.12	All records relating to the management of contracts under seal	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL	
2.5.13	All records relating to the management of contracts under signature	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL	
2.5.14	Records relating to the monitoring of contracts		Life of contract + 6 or 12 years	SECURE DISPOSAL	

2.5	Financial Management				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
School Fund					
2.5.15	School Fund - Cheque books		Current year + 6 years	SECURE DISPOSAL	
2.5.16	School Fund - Paying in books		Current year + 6 years	SECURE DISPOSAL	
2.5.17	School Fund – Ledger		Current year + 6 years	SECURE DISPOSAL	
2.5.18	School Fund – Invoices		Current year + 6 years	SECURE DISPOSAL	
2.5.19	School Fund – Receipts		Current year + 6 years	SECURE DISPOSAL	
2.5.20	School Fund - Bank statements		Current year + 6 years	SECURE DISPOSAL	
2.5.21	School Fund – Journey Books		Current year + 6 years	SECURE DISPOSAL	
School Meals Management					
2.5.22	Free school meals registers (where the register is used as a basis for funding)		Current year + 6 years	SECURE DISPOSAL	Yes
2.5.23	School meals registers		Current year + 3 years	SECURE DISPOSAL	Yes
2.5.24	School meals summary sheets		Current year + 3 years	SECURE DISPOSAL	Yes

978-1-9161239-1-5

2.6	Property Management				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
Property Management					
2.6.1	Title deeds of properties belonging to the school		These should follow the property unless the property has been registered with the Land Registry		
2.6.2	Plans of property belonging to the school		These should be retained whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold. See 2.4.10		
2.6.3	Leases of property leased by or to the school		Expiry of lease + 6 years	SECURE DISPOSAL	
2.6.4	Records relating to the letting of school premises		Current financial year + 6 years	SECURE DISPOSAL	
Maintenance					
2.6.5	All records relating to the maintenance of the school carried out by contractors		These should be retained whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold. See 2.4.10	SECURE DISPOSAL	
2.6.6	All records relating to the maintenance of the school carried out by school employees, including maintenance log books		These should be retained whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold. See 2.4.10	SECURE DISPOSAL	

3 Pupil Management

This section contains retention periods connected to the processes involved in managing a pupil's journey through school, including the admissions process.

3.1	Admissions Process				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
3.1.1	All records relating to the creation and implementation of the School Admissions Policy	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL	
3.1.2	Admissions – if the admission is successful	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL	Yes
3.1.3	Admissions – if the appeal is unsuccessful	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL	Yes
3.1.4	Register of Admissions	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made	REVIEW Schools may wish to consider keeping the admission register permanently as an archive record as often schools receive enquiries from past pupils to confirm the dates they attended the school or to transfer these records to the appropriate County Archives Service	

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
3.1.5	Admissions – Secondary Schools – Casual		Current year + 1 year	SECURE DISPOSAL	Yes
3.1.6	Proofs of address supplied by parents as part of the admissions process	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL	Yes
3.1.7	Supplementary information form including additional information such as religion, medical conditions etc.				Yes
3.1.7.1	For successful admissions		This information should be added to the pupil file	SECURE DISPOSAL	
3.1.7.2	For unsuccessful admissions		Until appeals process completed (GDPR)	SECURE DISPOSAL	

3.2	Pupil's Educational Record				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
Please note that any record containing pupil information may be subject to the requirements of the IICSA. Schools should implement any instruction which has been received from IICSA. The instructions from IICSA will override any guidance given in this Retention Schedule. If any school is unsure about what records should be retained, they should seek the advice of their own local authority or take independent legal advice.					
3.2.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437 As amended by SI 2018 No 688			Yes
3.2.1.1	Primary		Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • To another primary school • To a secondary school • To a pupil referral unit	
3.2.1.2	Secondary	Limitation Act 1980 (Section 2)	Date of birth of the pupil + 25 years	REVIEW	
3.2.2	Examination Results – pupil copies				Yes
3.2.2.1	Public		This information should be added to the pupil file	All uncollected certificates should be returned to the examination board after reasonable attempts to contact the pupil have failed	
3.2.2.2	Internal		This information should be added to the pupil file		

978-1-9161239-1-5

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
3.2.3	Child protection information held on pupil file	"Keeping children safe in education Statutory guidance for schools and colleges 2018"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file. Note: These records will be subject to any instruction given by IICSA	SECURE DISPOSAL These records must be shredded	Yes
3.2.4	Child protection information held in separate files	"Keeping children safe in education Statutory guidance for schools and colleges 2018"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record Note: These records will be subject to any instruction given by IICSA	SECURE DISPOSAL These records must be shredded	Yes

3.3 Attendance					
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
Please note that any record containing pupil information may be subject to the requirements of the IICSA. Schools should implement any instruction which has been received from IICSA. The instructions from IICSA will override any guidance given in this Retention Schedule. If any school is unsure about what records should be retained, they should seek the advice of their own local authority or take independent legal advice.					
3.3.1	Attendance Registers	School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of 3 years after the date on which the entry was made.	SECURE DISPOSAL	Yes
3.3.2	Correspondence relating to any absence (authorised or unauthorised)	Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL	Potential

3.3 Attendance					
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
Please note that any record containing pupil information may be subject to the requirements of the IICSA. Schools should implement any instruction which has been received from IICSA. The instructions from IICSA will override any guidance given in this Retention Schedule. If any school is unsure about what records should be retained, they should seek the advice of their own local authority or take independent legal advice.					
3.4.1	Special Educational Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Children and Family's Act 2014; Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 31 years [Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan in line with the Limitation Act]	SECURE DISPOSAL	Yes

978-1-9161239-1-5

4 Curriculum and Extra Curricular Activities

This section contains retention periods connected to the processes involved in managing the curriculum and extra-curricular activities.

4.1	Statistics and Management Information				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
4.1.1	Curriculum returns		Current year + 3 years	SECURE DISPOSAL	No
4.1.2	Examination Results (school's copy)		Current year + 6 years	SECURE DISPOSAL	Yes
4.1.2.1	SATS records				Yes
4.1.2.2	Results		The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all of the whole year's SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL	
4.1.2.3	Examination Papers		The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL	
4.1.3	Published Admission Number (PAN) Reports		Current year + 6 years	SECURE DISPOSAL	Yes

4.1	Statistics and Management Information				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
4.1.4	Value Added and Contextual Data		Current year + 6 years	SECURE DISPOSAL	Yes
4.1.5	Self-Evaluation Forms			SECURE DISPOSAL	Yes
4.1.5.1	Internal moderation		Academic year plus 1 academic year	SECURE DISPOSAL	Yes
4.1.5.2	External moderation		Until superseded	SECURE DISPOSAL	Yes
4.2	**Implementation of Curriculum**				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
4.2.1	Schemes of work		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL	
4.2.2	Timetable		Current year + 1 year		
4.2.3	Class record books		Current year + 1 year		
4.2.4	Mark books		Current year + 1 year		
4.2.5	Record of home-work set		Current year + 1 year		
4.2.6	Pupil's work		Where possible, the pupil's work should be returned to the pupil at the end of the academic year. If this is not the school's policy then current year + 1 year	SECURE DISPOSAL	

For information relating to records concerning the running of educational visits outside the classroom please see the guidance provided by https://oeapng.info/

978-1-9161239-1-5

4.3 School Trips					
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
4.3.1	Parental consent forms for school trips where there has been no major incident		Although the consent forms could be retained for Date of birth + 22 years, the school may wish to complete a risk assessment to assess whether the forms are likely to be required and could make a decision to dispose of the consent forms at the end of the trip (or at the end of the academic year). This is a pragmatic approach and if in doubt the achool should seek legal advice	SECURE DISPOSAL	Yes
4.3.2	Parental permission slips for school trips – where there has been a major incident	Limitation Act 1980 (Section 2)	Date of birth of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL	Yes

4.4	School Support Organisations				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
Family Liaison Officers and Home School Liaison Assistants					
4.4.1	Day books		Current year + 2 years then review	SECURE DISPOSAL	Yes
4.4.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency		Whilst child is attending school and then destroy	SECURE DISPOSAL	Yes
4.4.3	Referral forms		While the referral is current	SECURE DISPOSAL	Yes
4.4.4	Contact data sheets		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL	Yes
4.4.5	Contact database entries		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL	Yes
4.4.6	Group registers		Current year + 2 years	SECURE DISPOSAL	Yes
Parent Teacher Associations and Old Pupils Associations					
4.4.7	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations		Current year + 6 years then review	SECURE DISPOSAL	

978-1-9161239-1-5

5 Central Government and Local Authority

This section covers records created in the course of interaction between the school and local authority

5.1	Local Authority				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
5.1.1	Secondary Transfer Sheets (primary)		Current year + 2 years	SECURE DISPOSAL	Yes
5.1.2	Attendance returns		Current year + 1 year	SECURE DISPOSAL	Yes
5.1.3	School census returns		Current year + 5 years	SECURE DISPOSAL	
5.1.4	Circulars and other information sent from the local authority		Operational use	SECURE DISPOSAL	
5.2	**Central Government**				
	Basic file description	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of the administrative life of the record**	**Personal Information**
5.2.1	OFSTED reports and papers where a physical copy is held		Life of the report then review	SECURE DISPOSAL	
5.2.2	Returns made to central government		Current year + 6 years	SECURE DISPOSAL	
5.2.3	Circulars and other information sent from central govern-ment		Operational use	SECURE DISPOSAL	