Founded 1125

Policy number F8

Reading School

Data Policy

Storage of Personal Data and Privacy

Responsibilities

Policy Owner: Name, Jo Lidbetter
Title: Office Manager

Governors Committee Finance

Audit Control

Policy created: 22/06/2021
Date of next review June 2025
Version: 5.0
Statutory policy Yes

Data Policy

Document Control and Approval

Version Control

Version	Author	Summary of Changes	Reviewed By	Date
1.0	Jonathan Hitchinson	Policy created	Jonathan Hitchinson	01/05/2021
2.0	Jonathan Hitchinson	Updated information on photographs, videos	Jonathan Hitchinson	01/07/2022
3.0	Jonathan Hitchinson	Retention guidance added		14/09/22
4.0	Jo Lidbetter	DPO contact details updated		27/03/23
5.0	Jo Lidbetter	Statutory Provision Retention periods relating to disciplinary and grievance processes updated		21/04/23
5.0		Approved by Finance Committee		16/05/23
5.1		Artificial intelligence (AI) clause added		02/07/24

Responsibilities

Job title	Responsible for;
Office Manager	Policy Owner
Chief Operating Officer	Policy Overview
Finance Committee	Committee Responsible

Policies Linked

Policy name	File location

Forms Linked

Form name	Form location

Staff that need to sign

Staff Group	Form location

Contents

Data Protection

Aims

Reading School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format. 2. Legislation and guidance This policy meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR, the ICO's code of practice for subject access requests and guidance from the Department for Education (DfE) on Generative artificial intelligence in education

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. In addition, this policy complies with our funding agreement and articles of association.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is
	held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The data controller

Reading School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required

Roles and responsibilities

This policy applies to all staff employed by Reading School, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

- The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
- Full details of the DPO's responsibilities are set out in their job description.
- Our DPO is Satswana and is contactable viahttp://www.satswana.com.
- Their contact details are as follows:

Suite G12,Ferneberga House, Farnborough, Hampshire, GU14 6DQ; **Tel**: 01252 759177 **Email**: info@satswana.com

Headmaster

The headmaster acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in Chapter 2, sections 8 & 10 of the Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Retention Guidelines.

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

We may also transfer information to any association society or club set up for the purpose of maintaining contact with pupils or ex pupils and their parents/guardians or for fundraising, marketing or promotional purposes relating to the School, where consent has been obtained, make personal data, including special category data available to staff for the planning of school visits, curricular or extra-curricular activities, use photographs and moving images of pupils in accordance with the photograph procedures

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a ‘subject access request’ to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parental requests to see the educational record

There is no automatic parental right to access the educational record in an Academy. However, at Reading School, we will consider requests from parents. Parents should put a request in writing to the Headmaster. The school will respond within 15 school days.

Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash we will comply with the requirements of the Freedoms Act.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at

least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash to the Finance Office if they wish.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

Photographs and videos

For information on the taking, sharing and storage of photographs, videos, and for CCTV use, please refer to the Schools Taking, Storing and Using Images of Children Policy

Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Reading School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Reading School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E Safety Policy and ICT User Agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

Disposal of records

Data Policy

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Data Breach

Personal data breaches

Under GDPR, all organisations acting as data controllers must report security breaches involving personal data to the relevant supervisory authority if the breach is likely to result in a risk to individuals' rights and freedoms.

Such breaches must be reported without undue delay and, where feasible, within 72 hours of becoming aware of the breach. There is also a requirement to keep a record of such breaches.

While the GDPR is in relation to 'personal data', breaches involving any kind of data should also be reported internally and to appropriate personnel in accordance with this policy.

This policy should be considered in conjunction with:

- The internal data security policy.
- The management and retention of records policy.
- Personnel record keeping policy.
- The privacy notices.
- Data Policy.
- The ICT policies.
- Taking, Storing and Using Images of Children

Responsibilities

All employees, workers, governors, and consultants are responsible for reporting any data breaches they discover, or are responsible for, and for assisting in investigations where required.

Data breaches must be reported to the data protection officer (DPO) to consider what actions need to be taken with management and IT to address the incident, including whether to report the incident to the Information Commissioner's Office (ICO) and any affected individuals.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data. Broadly, it can be defined as a security incident that compromises the confidentiality, integrity or availability of personal data.

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error.
- Unforeseen circumstances, such as a fire or flood.
- Hacking attack.
- 'Blagging' offences where information is obtained by deceiving the organisation that holds it.

However, the breach has occurred, there are four important elements to any breach management plan:

- Containment and recovery.
- Assessment of ongoing risk.
- Notification of breach.
- Evaluation and response.

What are the school's responsibilities?

We process personal data on behalf of our pupils, their parents or guardians and all personnel connected within the school, including our staff and volunteers. Under the GDPR, we are classed as a 'data controller 'and we are therefore responsible for ensuring compliance with the various laws in place to protect individual privacy rights. We have privacy notices in place for the various categories of individuals whose data we process.

Where we engage third parties to process personal data on our behalf, such as payroll, we must also ensure that they process our data in a way that is compatible with the GDPR to ensure that the personal data is not compromised in anyway. We have set up arrangements to ensure that any third parties we engage, known as

'data processors', are GDPR compliant and have in place appropriate breach protocols and notification requirements.

While this policy is largely focused on personal data and our obligations under the GDPR, internal data and commercially sensitive data must likewise be protected and secure. Data breaches relating to any sort of data should be reported to the DPO.

What to do if you suspect there has been a data breach regarding personal data?

Data breaches could involve anyone's personal data that we process at the school. Do not investigate the matter yourself. Complete an incident form and pass it to the DPO. See appendix 1 for the data breach incident form. Due to the legal requirements of reporting personal data breaches within 72 hours, or such reasonable time, it is crucial that breaches are addressed immediately. Do not ignore them because the consequences may be worse, and can include substantial fines and penalties as well as personal repercussions for you.

If the breach involves the compromising of servers/IT security systems, you should also contact the IT department, so that immediate action can be taken to limit any damage/exposure.

What happens next?

Data breaches, whether they involve personal data or not, will be considered in line with our data breach protocol (appendix 2). You may be required to assist with the investigation process and/or help resolve any security incidents as part of your role.

Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- E Safety Policy
- Privacy Notices
- Child Protection Policy
- Safeguarding Policy
- ICT User Agreement

Appendix

Data Breach Incident Form

Description of the data breach		
Time and date the breach was identified and by whom	Time	Date
Who is reporting the breach	Name	Job Title
Contact details	Mobile	Email
Classification of data breached • Personal data • Internal data • Confidential data • Highly confidential data • Commercial data		
Volume of data involved		
Confirmed or suspected breach?		
Is the breach contained or ongoing?		
Who has been informed of the breach?		
Any other information		

Data Breach Protocol

This protocol sets out what we need to do in the event of a data breach. Stage one below is covered by the data breach policy. However, stages two to four will be carried out by the DPO with appropriate support from other personnel, such as IT support and the DPM.

The data breach protocol comprises four stages

- Incident report to the DPO.
- Containment and recovery/investigation and assessment of data breach.
- Consideration of reporting requirements to ICO/individual.
- Evaluation and response, record of breach kept, consideration of any additional security measures needed.

Stage one – incident report

Any data breaches must be reported to the DPO immediately in line with the data breach policy above.

Stage two – containment and recovery/investigation and assessment

Containment and recovery

Depending on the type of breach incident, it may be appropriate to take immediate steps to contain the threat or recover the data. Consult with IT and management.

The requirement to report breaches to individuals in high-risk cases may require the DPO to notify individuals whose personal data has or may have been compromised of the situation straightaway. This consideration should be kept under constant review throughout the process.

Any 'data processor' breaches by any of the third parties we engage should also be reported to us to enable us to take appropriate action.

Investigation and assessment

Investigating the incident will involve:

- Considering the incident report.
- Discussing matters with appropriate personnel and obtaining relevant reports/statements.
- Finding out what has happened and what data is affected.
- Consideration of whether the data is high risk, commercially sensitive or includes personal data/special categories of personal data.
- Keeping a timeline/log and updating the developments of the breach.
- Consideration of whether, in the case of personal data, the breach affects the fundamental rights and freedoms of the data subject with regard to:
- Any resulting physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights,

discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned

- The severity of the breach generally.

Stage three – breach reporting

Given the length of time that incidents have to be reported by, it may be appropriate to report the incident without having fully investigated the issues. Matters may develop, and a log should be kept as they do.

If the breach does impact on the rights and freedoms of the data subject(s), report the breach to the ICO if appropriate at https://ico.org.uk/for-organisations/report-a-breach.

Notify any data subject of the personal data breach if appropriate where there is a high risk and without undue delay. This will allow the data subject to mitigate any immediate risks of damage. Notification should include:

- Details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the breach including any measures to mitigate any possible adverse effects.

Consideration must be given to whether our insurers need to be informed.

Stage four – evaluation and response

The final breach report should include a summary of the facts of the breach, its effects and the remedial action we have taken. Consideration of whether the issue is human error or not and how reoccurrence can be prevented

Founded 1125

Reading School

Personal Data

Retention Guidelines and Data Destruction

Governing Body

This section contains retention periods connected to the work and responsibilities of the governing body.

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
1.1	**Management of Governing Body**				
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
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 avail- able for 10 years from the date of the meeting	Consult local archives before disposal	Potential
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

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
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 re- quired 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	
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 ad- ministered 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**				
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,		Date appointment ceases + 6 years		Yes

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
	including evidence of appointment				
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
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

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.

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
2.1	**Head Teacher and Senior Management Team**				
2.1.1	Logbooks of activity in the school maintained by the Head Teacher		Date of last entry in the book + mini- mum 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
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	

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
2.2	**Operational Administration**				
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**				
• **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

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
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
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 online 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
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.	SECURE DISPOSAL	Yes
			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 cur- rent year + 3 years as being		

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
			acceptable as this gives them, 'benefits' and Inland Revenue have time to investigate if they need to		
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
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 safe- guard 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
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					

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
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 + 12 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 + 12 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file	
	Written warning – level 2		Date of warning + 12 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file	
	Final warning		Date of warning + 18 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file	
	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	
• **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

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
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
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
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

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
2.3.33	Pension payroll	Taxes Management Act 1970 Income and Corporation Taxes 1988	Current year + 6 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
	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

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
2.4	**Health and Safety**				
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 Ad- ministration 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 se- cure with restricted access. Data Protection Act 2018 and GDPR	SECURE DISPOSAL	Yes

	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
2.4.6	Control of Substances Hazardous to Health (COSHH)	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677	Date of incident + 40 years	SECURE DISPOSAL	

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
		Regulation 11; Records kept un- der the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)			
2.4.7	Process of monitoring of areas where employees and persons are likely to have come into con- tact 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 logbooks		Current year + 3 years	SECURE DISPOSAL	
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**				
• **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	

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
• **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	
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

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
• **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	
2.5.15	School Fund - Cheque books		Current year + 6 years	SECURE DISPOSAL	
• **School Fund**					
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

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
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
2.6	**Property Management**				
• **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 logbooks		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	

Pupil Management

This section contains retention periods connected to the processes involved in managing a pupil's journey through school, including the admissions process.

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
3.1	**Admissions Process**				
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	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	

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
		admission appeals panels December 2014		appropriate County Archives Service	
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**				
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	

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
				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		
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
3.4	**Special Educational Needs**				
3.4.1	Special Educational Needs files, reviews and Education, Health and Care Plan, including ad- vice 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

Curriculum and Extra Curricular Activities

This section contains retention periods connected to the processes involved in managing the curriculum and extra-curricular activities.

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
4.1	**Statistics and Management 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
4.1.4	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

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
4.2	**Implementation of Curriculum**				
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/					
4.3	**School Trips**				
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 school 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
4.4.1	Day books		Current year + 2 years then review	SECURE DISPOSAL	Yes

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
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	**School Support Organisations**				
• **Family Liaison Officers and Home School Liaison Assistants**					
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	
4.4.8	Reading School's Alumni Society		Current year, will retain some personal data of historic value, including photographs, school photographs, historical pupil lists and may be archived in perpetuity	SECURE DISPOSAL	Yes

Central Government and Local Authority

This section covers records created in the course of interaction between the school and local authority

	Basic file description	Statutory Provisions	Retention Period [Operational]	Action at end of the administrative life of the record	Personal Information
5.1	**Local Authority**				
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**				
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 government		Operational use	SECURE DISPOSAL	

Data retention justification examples

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long-term need (until pupil is aged 25 or older)	Justification
Admissions		X (admissions files)	X (admissions appeal)		**Admissions files** Admissions data is used extensively from the period of the school receiving it up until the point where children enrol. It is then used for some validation and cross checking of enrolment details. Once enrolled, the child's records in the MIS become the core record. Data about children who enrolled but didn't get in is useful, but any intelligence gathered from it (for example, where in the city children are interested in our school, or the SEN make up) is aggregated within the first year to a level being non-personal, after that, the detailed data within the admission file could be deleted . It is important to retain detailed data for a year, any appeals for which richer data about other successful/unsuccessful appeals may be relevant typically happen in the first year. **Information about admissions appeals** When dealing with appeals, having a reasonable history of any other appeals in some detail can be needed to deal with the particular appeal. The information is needed alongside the admissions policies of the time.
Attainment			X		**Formative assessment** data is useful as a child is building towards a particular more formal assessment. Once the child leaves the school, it has little value in terms of retention. **Summative attainment** is the main outcome of what children 'attain' in school. It is important that future schools where pupils go on to learn can understand previous attainment. Whilst often that information is 'passed on' smoothly as children move phase, it is not always the case, and thus retaining the names alongside the main attainment data for 1 year after the pupil has left the school feels proportionate.

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long-term need (until pupil is aged 25 or older)	Justification
					Trend analysis is important, 3 to 5 years is often the 'trend' people look at, but longer may be relevant. Whilst this must be fully flexible in reporting small sub groups, and the data would wish to be retained at individual level, some personal data (for example, name) could be removed from the data to reduce sensitivity. After 3 to 5 years, then aggregated summaries that have no risk of identifying individuals are all that are typically needed to be retained.
Attendance		X			Attendance data probably resides in some 'operational' systems in schools, such as cashless catering. In these systems, the data should only be retained until the associated business processes have concluded (for example, payment of meals). The start of the next academic year once all bills are settled feels proportionate. Attendance is related to individual attainment and so being able to relate attendance to attainment whilst in our care is important. Keeping it in detailed, individual form for one year after the pupil leaves school support conversations about detailed attendance that may be needed to best support that child. After that period, non-identifiable summary statistics are all that is required to support longer- term trend analysis of attendance patterns. We noted another GDPR principle here that may apply to attendance. Under data minimisation, where 'paper records' capture attendance, this paper record duplicates the electronic version and is probably required once the paper has been transferred to a stable electronic format.
Behaviour		X			This is all relevant for managing children when with at your school. 1 year allows a period of 'handover' to next institution with conversations supported by rich data if relevant.
Exclusions		X			Exclusion data should be 'passed on' to subsequent settings. That school then has responsibility for retaining the full history of the child. If a private setting or the school is unsure on where the child has gone, then the school should ensure the LA already has the exclusion data.

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long-term need (until pupil is aged 25 or older)	Justification
Identity management and authentication	X (images used for identity management)				
Catering and free school meal management		X (meal administration)	X (free school meal eligibility information)		A short historic record of what a child has had may be useful in case of any food-related incidents at school, or parental queries about the types of meals their children are choosing. Keeping for up to one year also allows time to do accounting work associated with catering. Typically, 'one month' may not be enough, but 'one year' feels enough. Due to the way school funding works, free school meal eligibility is a financial matter, and thus keeping this data for 6+1 feels appropriate. This 7- year record also needs to be portable with the pupil, as historic dates can be used for funding.
Trips and activities	X (field file) X (educational visitors into school)		X (financial information related to trips)	X (major medical events)	**Financial information** related to trips should be retained for 6 years + 1 for audit purposes. This would include enough child identifiers to be able to confirm contributions. A '**field file'** is the information that is taken on a trip by a school. This can be destroyed following the trip, once any medicines administer on the trip have been entered onto the core system. If there is a minor medical incident on the trip (for example, a medical incident dealt with by staff in the way it would be dealt with 'within school'), then adding it into the core system would be done. If there is a major incident (for example, a medical incident that needed outside agency) then retaining the entire file until time that the youngest child becomes 25 would be appropriate. Permission to go on the trip slips will contain personal data, and destroying them after the trip unless any significant incident arises is appropriate, otherwise refer to the policies above. Schools sometimes share personal data with people providing 'educational visits' into school. There should be good policies in place to ensure that the sharing is proportionate and appropriately deleted afterwards.

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long-term need (until pupil is aged 25 or older)	Justification
Medical information and administration	X (permission slips)	X (medical conditions and ongoing management)		X medical incidents (potentially)	To support any handover work about effective management of medical conditions to a subsequent institution. Permission forms that parents sign should to be retained for the period that medication is given, and for 1 month afterwards if no issue is raised by child/parent. If no issue is raised in that time, that feels a reasonable window to assume all was administered satisfactorily. Adding this policy to the permission slip would seem prudent. Medical 'incidents' that have a behavioural or safeguarding angle (including the school's duty of care) should refer to the retention periods associated with those policies.
Safeguarding				X	All data on the safeguarding file potentially forms part of an important story that may be needed retrospectively for many years. The elements of a pupil file (name, address) that are needed to identify children with certainty are needed to be retained along with those records.
Special educational needs					Refer to IRMS toolkit
Personal identifiers, contacts and personal characteristics	X (images used in identity systems) X (biometrics) X (house number and road	X (images used in displays in school)	X (postcodes) X (names) X (characteristics)		Images are used for different reasons, and the reason should dictate the retention period. Images used purely for identification can be deleted when the child leaves the setting. Images used in displays etc. can be retained for educational purposes whilst the child is at the school. Other usages of images (for example, marketing) should be retained for and used in line with the active informed consent, captured at the outset of using the photograph. Biometric data (typically fingerprints used in things like catering) should be used and retained as set out in the active informed consent gained at the outset, but typically this should not be retained long after the activity that requested its use has finished (for example, the child no longer attends the school to have a meal). As set out in other sections, names are needed for smooth handover to subsequent schools for up to one year.

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long-term need (until pupil is aged 25 or older)	Justification
					Postcode data is useful in analysing longer-term; performance trends or how catchment/pupil populations are shifting over time, but full address data (house number and road) is not required for that activity. Schools may well provide references for pupils for up to 3 years after they leave, and so retaining the name in the core pupil record is important (this doesn't mean it needs to be retained in all systems). Keeping names attached to safeguarding files for longer than this may be entirely appropriate – see safeguarding section. Characteristics form an essential part of trend analysis, and so retention is in line with those needs.