



Data Protection and Retention Policy

Date reviewed and approved by Governing Body: December 2025

Review period: Annually

Next review due: November 2026

Model Policy  updated August 2025

Contents

1.	Aims	2
2.	Legislation and guidance	2
3.	Definitions	2
4.	The data controller	3
5.	Roles and responsibilities	3
6.	Data protection principles	4
7.	Collecting personal data	4
8.	Sharing personal data	6
9.	Subject access requests and other rights of individuals	6
10.	Parental requests to see the educational record	8
11.	CCTV	8
12.	Photographs and videos	8
13.	Artificial Intelligence (AI)	9
14.	Data protection by design and default	9
15.	Data Retention (this section was previously Appendix B)	10
16.	Data security and storage of records	11
17.	Disposal of records	11
18.	Training	12
19.	Monitoring arrangements	12
20.	Equality Review	12
21.	Links with other policies	12
	Appendix A: Data Retention	13
	Appendix B: Personal Data Breach Procedure	19

1. Aims

Our 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 UK data protection law.

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 General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Data Protection Act 2018 \(DPA 2018\)](#)
- [References: Data \(Use and Access\) Act 2025: data protection and privacy changes - GOV.UK](#) and [The Data Use and Access Act 2025 \(DUAA\) - what does it mean for organisations? | ICO](#) (introduced June 2025)

It is based on guidance published by the Information Commissioner's Office (ICO) on [The UK GDPR | ICO](#) and guidance from the Department for Education for Education (DfE) on [Generative artificial intelligence in education](#)

It also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information. Additional information around CCTV and organisational arrangements is available [here](#).

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's Educational Record: [Accessing pupils' information | ICO](#).

3. Definitions

TERM	DEFINITION
Personal data	<p>Any information relating to an identified, or identifiable, living individual. This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">• Racial or ethnic origin• Political opinions• Religious or philosophical beliefs• Trade union membership

	<ul style="list-style-type: none"> • 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.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required. For reference, please check the following link: [Register of fee payers and certificate downloads | ICO](#)

5. Roles and responsibilities

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

Governing body - has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

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.

For routine enquiries about this policy, contact the School Business Manager who is the school's data protection representative via finance@littlepaxton.cambs.sch.uk

The DPO is also a point of contact for individuals whose data the school processes, and the first point of contact for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is **The ICT Service** and is contactable via dpo@theictservice.org.uk

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

All 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

6. 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.

7. 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 or another person i.e. 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 or exercise its official authority
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) 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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them

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 to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

Please refer to Item 17 which links to our school's retention arrangements.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 contract with the supplier or contractor 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

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

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.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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

- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form, they must immediately forward it to the School Business Manager on finance@littlepaxton.cambs.sch.uk

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 below the age of 13 are generally not 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 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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent, and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 contact the school's data protection representative via finance@littlepaxton.cambs.sch.uk. If other staff receive such a request, they must immediately forward it to the school's data protection representative who will liaise with the DPO as required.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the [guidance](#) for the use of and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to School Business Manager, via finance@littlepaxton.cambs.sch.uk. Please also refer to the CCTV policy.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13. 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. Little Paxton Primary 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, Little Paxton Primary School will treat this as a data breach and will follow the personal data breach procedure outlined in Appendix 1.

14. Data protection by design and default

We will put the following 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 data protection 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 agendas and

attendance at training days. Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.

- Appropriate safeguards being put in place if we transfer any personal data outside of the United Kingdom, where different data protection laws will apply. (Where applicable).

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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the United Kingdom and the safeguards for those, retention periods and how we are keeping the data secure.

15. Data Retention (this section was previously Appendix B)

Little Paxton Primary 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.

Little Paxton Primary School undertakes to manage records in relation to the three principles laid out in the Lord Chancellor's Code of Practice issued under Section 46 of the Freedom of Information Act 2000, published in July 2021.

This policy provides the framework to achieve effective management and audit of records. It covers:

- Scope
- Responsibilities

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

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.

The governing body has a statutory responsibility to maintain the 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.

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.

Information will be managed 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').

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

- Manage the school's records consistently in accordance with the school's policies and procedures.
- Properly document their actions and decisions.
- Hold personal information securely.
- Only share personal information appropriately and do not disclose it to any unauthorised third party.
- Dispose of records securely in accordance with the school's Records Retention Schedule.

Information will be assessed and when it is no longer required, necessary or is to be destroyed or deleted in line with the retention schedule.

The security of data and appropriate measures will be implemented to protect breach, loss or unauthorised sharing of the information.

16. 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 secure when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops.
- 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 ICT acceptable use policy)

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)

17. Disposal of records

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 use an external contractor safely to dispose of paper records on the school's behalf. Electronic devices are disposed of via a third party who confirm files have been deleted. We require the third party to provide sufficient guarantees that it complies with data protection law, they do this by issuing us with a certificate of destruction.

All data will be kept in accordance with our Retention Schedule.

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix C.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- 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

18. 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.

19. Monitoring arrangements

The Headteacher and DPO are responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

20. Equality Review

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this school.

21. Links with other policies

This data protection policy is linked to our:

- Safeguarding and Child Protection Policy
- Code of Practice
- ICT and Internet Use Policy
- CCTV Policy

Appendix A: Data Retention

Retention of Staff Personal Data

This schedule lists the principal documents held on an employee's file. The list is not exhaustive, and other documents relating to employment may be also held. Personnel files will be held for the length of employment + 6 years at which time they will be securely shredded. Documents relating to child protection or accidents at work may be held for a period of up to 25 years, in accordance with the DFE "Data protection: a toolkit for schools" and the employee will be advised of this.

Document	Period of Retention <i>Recommended unless stated</i>
Application Process	
Application forms and interview notes (for unsuccessful candidates)	One year
Original job application form for successful candidate	Termination + 6 years
Documents Relating to Appointment Process <i>**Recommended within the DFE guidance, 'Data Protection: a toolkit for schools', February 2023</i> <i>^ Recommended within Home Office 'An Employers Guide to Right to Work Checks', September 2024</i>	
Confirmation of pre-employment medical check clearance	Termination + 6 years
DBS certificates/copies <i>*If retained, maximum period six months and if, in very exceptional circumstances, it is considered necessary to retain a copy of the original certificate for longer than six months, consent should be sought from the applicant and retained on file.</i>	No requirement to retain*
Confirmation of DBS outcome and any associated docs (e.g. risk assessment or certificate of good conduct) **	Termination + 25 years
Barred list clearance **	Termination + 25 years
Prohibition check **	Termination + 25 years
Copies of documents used for identity authentication for DBS and Asylum and Immigration Act purposes^	Termination + 2 years
UK Border Agency Documentation (Work permit) ^	Termination + 2 years
Records relating to employees from outside of the UK e.g. visa, work permits, etc. ^	Termination + 2 years
Copies of qualifications certificates relevant to employment	Termination + 6 years
NQT – Satisfactory completion of skills tests.	Termination + 6 years
Two original references	Termination + 6 years
Original contract acceptance	Termination + 6 years

Copy of Contract of employment and any variation letters or side letters	Termination + 6 years
Disciplinary Records	
Formal disciplinary warnings – child protection related **	Termination + 25 years
Formal disciplinary warnings – not child protection related	Termination + 6 years
Accidents at Work	
Accident books, accident records, accident reports	Three years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches age 21) <i>Statutory</i>
Records relating to accident/injury at work	Termination + 12 years In the case of serious accidents, a further retention period may need to be considered
Financial Information	
Inland Revenue/HMRC correspondence	Termination + 6 years <i>Statutory</i>
National minimum wage records	Three years after the end of the pay reference period following the one that the records cover. <i>Statutory</i>
Wage/salary records (also overtime, bonuses, expenses)	Termination + 6 years <i>Statutory</i>
Time sheets	Current year + 6 years
Sickness and Maternity Information	
Medical certificates/Occupational Health reports and sickness absence record	Current year + 6 years
SMP, SAP, SSPP records, calculations, certificates (Mat B1s) or other medical evidence, notifications, declarations and notices	Three years after the end of the tax year in which the leave period ends <i>Statutory</i>
Statutory Sick Pay records, calculations, certificates, self-certificates	Six years after the employment ceases
Parental leave records	Eighteen from birth/adoption of the child or if the child receives a disability living allowance
Other special leave of absence including parental leave, maternity leave	Current year + 6 years
Leavers Information	

Letter of resignation and acceptance of resignation or other documentation relating to the termination of employment	Termination + 7 years
Exit interview notes	Termination + 7 years
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	Six years from the date of redundancy
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	Six years from the end of the scheme year in which the event took place <i>Statutory</i>
Additional Employee Information	
Salary assessment forms – teachers	Current year + 6 years
Appraisal information	Current year + 6 years
Staff induction including ECTs Induction <i>Recommended within DFE statutory guidance ‘Induction for Early Career Teachers (England), April 2023</i>	Completion + 6 years
Working time records	Two years from date on which they were made <i>Statutory</i>
Personnel files and training records (including disciplinary records)	Six years after employment ceases Recommended retention period <i>(non-statutory) Chartered Institute of Personnel</i>
Records of any reportable death, injury, disease, or dangerous occurrence	Three years after the date record was made Requirement: The reporting of Injuries, Disease and Dangerous occurrences regulations 1995 (RIDDOR) (as amended)

Retention of Pupil Personal Data

<https://www.cambslearntogether.co.uk/cambridgeshire-early-years-and-childcare/business-and-governance/gdpr>

Record	Retention period	Statutory Authority/Non-Statutory recommendation
Nursery Education Funding Scheme	Seven years	Statutory requirement Local Authority
Children's records which would include attendance records, registers, medication records/accident (Include staff records too)	All children's records must be kept while the child is in attendance at the setting and recommended for at least 3yrs after the child has left the provision <i>However settings must check with their insurance company about their particular requirement</i>	EYFS Statutory requirement 2017 <i>3.71 Records relating to individual children must be retained for a reasonable period of time after they have left the provision 56. Individual providers should determine how long to retain records relating to children</i> The Data Protection Act 1998/GDPR 2018 does not specify periods for the retention of personal data. It is left to data controllers to decide how long personal data should be retained, taking into account the Data Protection Principles (see Data Protection Act Overview/GDPR principles), business needs, and any professional guidelines
Child Welfare Records <i>Advise settings if sibling attends to keep a copy of records if they have ongoing concerns until sibling leaves the setting/starts school/new setting</i>	Transferred to the new setting/school with the child when they leave the setting. If the new setting/school is unknown, then the setting is to retain for 6 years from the date of the last entry and then archive until the child reaches 25 years old	The Independent Inquiry into Child Sexual Abuse requires all institutions to retain their records relating to the care of children for the duration of the Inquiry under Section 21 of the Inquiries Act 2005 . There is therefore an obligation to preserve records for the Inquiry for as long as is necessary. The Data Protection Act 1998/GDPR 2018 does not specify periods for the retention of personal data. It is left to data controllers to decide how long personal data should be retained, taking into account the Data Protection Principles (see Data Protection Act Overview/GDPR principles), business needs, and any professional guidelines. Primary school – These are retained while the child is in the school; then transfer to

		the relevant secondary school. Secondary school – These are retained until the child is 25 years old and then shredded
Complaints Records	Recommended at least six years from the date of the last record	EYFS Statutory Requirement 2021 IRMS irms.org.uk
Personnel files and training records (including disciplinary records and working time records)	Six years after employment ceases	Recommended retention period (non-statutory) Chartered Institute of Personnel
Accident/medical records as specified by The Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	Requirement The Control of Substances Hazardous to Health Regulations 2002 (COSHH)
Visitors books/signing-in sheets	The current year plus six years	Recommendation IRMS irms.org.uk
Fire Drill records	Recommend from date of last Ofsted inspection	Early Years Foundation Stage Framework 3.56 Providers must take reasonable steps to ensure the safety of children, staff, and others on the premises in the case of fire or any other emergency and must have an emergency evacuation period.

Retention of Other Personal Data

Record	Retention period	Statutory Authority/Non-Statutory recommendation
Accounting records	Six years for public limited companies and charities this should include the current year of trading	Statutory requirement Section 221 Companies Act 1985 Statutory requirement Charities Act 1993 (amended 2006)
Insurance liability documents	40 years from the date of expiry	Statutory requirement The Employers' Liability (Compulsory Insurance) Regulations 1998 Health and Safety executive hse.gov.uk
Records of any reportable death, injury, disease, or dangerous occurrence	Three years after the date record was made	Requirement: The reporting of Injuries, Disease and Dangerous occurrences regulations 1995 (RIDDOR) (as amended)
Accident/medical records as specified by The Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	Requirement The Control of Substances Hazardous to Health Regulations 2002 (COSHH)
Visitors books/signing-in sheets	The current year plus six years	Recommendation IRMS irms.org.uk
Fire Drill records	Recommend from date of last Ofsted inspection	Early Years Foundation Stage Framework 3.56 Providers must take reasonable steps to ensure the safety of children, staff, and others on the premises in the case of fire or any other emergency and must have an emergency evacuation period.

Appendix B: Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the schools data controller (School Business Manager) or the DPO
- The school's data protection representative and DPO will investigate the report and determine whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:
 - Lost.
 - Stolen.
 - Destroyed.
 - Altered.
 - Disclosed or made available where it should not have been.
 - Made available to unauthorised people.
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- The school's data protection representative and DPO will alert the Headteacher and the Chair of Governors.
- The school's data protection representative and the DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The data protection representative and DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.
- The data protection representative and DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The school's data protection representative and DPO will document the decision (either way), in case it is challenged at a later date by the ICO, or an individual affected by the breach. Documented decisions are stored on the school's computer network.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned.

- The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
 - A description, in clear and plain language, of the nature of the personal data breach
 - The name and contact details of the DPO.
 - A description of the likely consequences of the personal data breach.
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The school's data protection representative will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies.
- The school's data protection representative will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer network in an appropriate log format.

- The school's data protection representative and DPO will review what happened and how it can be stopped from happening again. This review will happen as soon as reasonably possible.
- The school's data protection representative and Headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce the risk of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the school's data protection representative as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the school's data protection representative will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system.

- In any cases where the recall is unsuccessful, the school's data protection representative will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save, or replicate it in any way.
- Other types of breach that you might want to consider could include:
 - Details of pupil premium interventions for named children being published on the school website.
 - Non-anonymised pupil exam results or staff pay information being shared with governors.
 - A school laptop containing non-encrypted sensitive personal data being stolen or hacked.
 - The school's cashless payment provider being hacked, and parents' financial details stolen.
 - Hardcopy reports sent to the wrong families.