Data Protection Policy

Model Policy epm

Date reviewed and approved by Governing Body: December 2023

Review period: Annually

Next review due: November 2024

Contents

1. Aims

1.1. 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.

1.2. 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:

1.1. 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

1.2. Data Protection Act 2018 (DPA 2018)

1.3. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

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

1.5. 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.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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.

4. The data controller

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

4.2. The school is registered with the ICO as legally required.

5. Roles and responsibilities

5.1. 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.

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

5.3. 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.

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

Our data protection officer is Donna J Flynn who can be contacted by email dpo@theictservice.org.uk, phone 0300 300 0000 option 1 or in writing Speke House, 17 Compass Point Business Park, Stocks Bridge Way, St Ives, Cambs PE27 5JL

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

5.5. 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

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

6.2. The principles say that personal data must be:

6.3. Processed lawfully, fairly and in a transparent manner

6.4. Collected for specified, explicit and legitimate purposes

6.5. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

6.6. Accurate and, where necessary, kept up to date

6.7. Kept for no longer than is necessary for the purposes for which it is processed

6.8. Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

Lawfulness, fairness and transparency

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

7.2. 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

7.3. The data needs to be processed so that the school can comply with a legal obligation

7.4. The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life

7.5. 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

7.6. 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

7.7. The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

7.8. For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

7.9. The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent

7.10. The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law

7.11. 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

7.12. The data has already been made manifestly public by the individual

7.13. The data needs to be processed for the establishment, exercise or defence of legal claims

7.14. The data needs to be processed for reasons of substantial public interest as defined in legislation

7.15. 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

7.16. 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

7.17. 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

7.18. 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

7.19. 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.

7.20. 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.

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

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

7.23. In addition, 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 record retention schedule.

8. Sharing personal data

8.1. 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:

8.2. There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

8.3. We need to liaise with other agencies – we will seek consent as necessary before doing this

8.4. 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

9.1. 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

9.2. Please see Appendix A for details of the procedure for Subject Access Requests.

9.3. If staff receive a subject access request in any form they must immediately forward it to the DPO.

Children and subject access requests

9.4. 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.

9.5. Children below the age of 12 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

9.6. 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

9.7. 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 take into account whether the request is repetitive in nature when making this decision.

9.8. 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

9.9. 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)
- 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.

10. Parental requests to see the educational record

10.1. 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.

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

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

10.4. 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

11.1. We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

11.2. 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.

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

12. Photographs and videos

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

12.2. 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.

12.3. 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.

12.4. 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

12.5. 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.

12.6. 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. Data protection by design and default

13.1. We will put the following measures in place to show that we have integrated data protection into all of our data processing activities:

13.2. Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

13.3. 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)

13.4. 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)

13.5. Integrating data protection into internal documents including this policy, any related policies and privacy notices

13.6. 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.

13.7. Annual reviews and audits to test our privacy measures and make sure we are compliant. Scheduled by the Head Teacher and School Business Manager.

13.8. Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply

13.9. 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 EEA and the safeguards for those, retention periods and how we are keeping the data secure. This is part of the GDPR data register process.

14. Data security and storage of records

14.1. Appendix B details our retention protocol, which follows recommended or statutory periods of retention.

14.2. 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.

14.3. Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept secure when not in use

14.4. 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

14.5. Where personal information needs to be taken off site, staff must sign it in and out from the school office

14.6. Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites

14.7. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

14.8. 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)

14.9. 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)

15. Disposal of records

15.1. 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.

15.2. 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.

16. Personal data breaches

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

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

16.3. 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:

16.4. A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

16.5. Safeguarding information being made available to an unauthorised person

16.6. The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

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

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

18. Monitoring arrangements

18.1. This policy will be reviewed every year and shared with the full governing body

19. Equality Review

19.1. 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.

19.2. 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.

20. Links with other policies

This data protection policy is linked to our:

- Code of Practice
- ICT and Internet Use Policy
- CCTV Policy

Appendix A: Subject Access Request Procedure

The UK General Data Protection Regulation

The General Data Protection Regulation (GDPR), which was brought into EU law in May 2016, has been retained in domestic law as the UK GDPR and sits alongside the amended version of the Data Protection Act 2018. It incorporates the GDPR into UK data protection law meaning that in practice there is little change to the core data protection principles, rights and obligations found in the GDPR.

UK GDPR entitles individuals to request access to any personal data that [name] is holding about them. This is known as a 'Data Subject Access Request.' This document is intended to give employees a guide to making a Data Subject Access Request (DSAR) and to what happens in processing DSARs.

A Data Subject Access Request (a 'DSAR') is where an individual, using their rights under UK GDPR makes a request for a copy of the personal data an organization holds on them, or details of what data is held and its source. A Data Subject Access Request does not have to reference UK GDPR, the term "Data Subject Access Request" or reference any legislative rights.

The Process

All DSAR's must be made in writing to our Data Protection Officer, contact details given below.

Where a request is received from elsewhere in the business, the Data Protection Officer should be immediately informed so they are able to deal with the request with no undue delay.

Once the request is received the Data Protection Officer will confirm the identity of the subject and assess the scope of the request. Once the identity of the data subject (or the right/authority to request the data where the data subject is not the requester) the Data Protection Officer will begin the process of contacting the appropriate departments to collect and collate the information. To locate the correct information within Little Paxton Primary School, the Data Protection Officer may ask the subject to confirm exactly what information they are requesting, or where they believe the information may be stored. Where the request is deemed to be 'manifestly unfounded or excessive', Little Paxton Primary School may charge a reasonable fee or refuse to respond to the request. This will be confirmed to the data subject in writing.

The information provided in reply to a request must be that which Little Paxton Primary School holds (subject to any exemptions) at the time the request is received. However, the Act allows routine updating and maintenance of the data to continue between the date on which the request is received and the date when the reply is dispatched. This means that the information provided to the individual may differ from that which was held at the time when your request was received, but only because of normal processing. Data cannot be deleted.

The Data Protection Officer will contact any third parties (e.g. authors of e-mails/letters contained within the file) in order to obtain consent to disclose the information to the subject. Where consent cannot be obtained or is denied the Data Protection Officer will consider the reasons and [name's] duty of care to both parties to decide whether to disclose the information. Where the information contains reference to third parties the Data Protection Officer will redact (blank out) the third parties. Where this is impossible and consent from the third party has not been received the information will not be disclosed.

All requests will be dealt with within one month of receipt (minus any time spent verifying identity or authorisation to act on the subject's behalf). The information will be dispatched to the subject as soon as the above process is complete.

Contacts & Complaints

Any enquiries regarding this procedure or Little Paxton Primary School Data Protection Policies should be directed to:

Data Protection Officer (DPO):	Donna J Flynn
Email:	dpo@theictservice.org.uk
Phone:	0300 300 0000 option 1
Postal Address:	Speke House, 17 Compass Point Business Park, Stocks Bridge Way, St Ives, Cambs PE27 5JL

If you require more information about the UK General Data Protection Regulation, the Data Protection Act 2018, or are unhappy with the way our Data Protection Officer has dealt with your request please contact:

The Information Commissioner
Wycliffe House, Water Lane, Wilmslow
Cheshire SK9 5AF

www.ico.org.uk

Appendix B: Data Retention Protocol

Introduction

This policy applies to all employees, workers and contractors.

The Governing Body/Trustees of Little Paxton Primary School are committed to retaining personal data (which may be held on paper, electronically, or otherwise) about our employees for no longer than necessary for the purpose or purposes for which they were collected. All steps will be reasonably taken to securely destroy or erase from systems, all data which is no longer required.

The Governing Body/Trustees recognise the need to process data in an appropriate and lawful manner, in accordance with the UK General Data Protection Regulation (UK GDPR). The purpose of this policy is to set out the principles by which we will retain your personal data.

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action, including dismissal.

The Head Teacher is responsible for ensuring compliance with the UK GDPR and this policy. Any questions about the operation of this policy or concerns that there has been a breach of this policy should be referred in the first instance to the Head Teacher.

Responsibilities

The Governing Body/Trustees understand their legal responsibility to comply with the law, including the UK General Data Protection Regulation. The individual with overall responsibility for this policy is the Data Protection Officer.

Retention of Data

The Governing Body/Trustees will state the purposes for which it holds personal information and will register with the Data Protection Commissioner all the purposes for which it processes personal data.

Personal data will be retained for employment purposes, to assist in the running of the business and/or to enable individuals to be paid. In such cases we will apply the 'recommended' retention period. Some personal data is retained for statutory purposes, in which case we will apply the 'statutory' retention period.

The Governing Body/Trustees commit to retaining the minimum amount of personal data that is necessary for the purpose for which it is held and access to the personal data will be restricted so that it is used only for the specific purpose.

Personal data will be held as indicated in Appendix 1 and for no longer than the period specified below. All personal data will be destroyed securely at the end of the retention period.

Retention of 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 *Recommended unless stated*
Application Process	
Application forms and interview notes (for unsuccessful candidates)	Six months
Original job application form for successful candidate	Termination + 6 years
Documents Relating to Appointment Process	
Confirmation of pre-employment medical check clearance	Termination + 6 years
DBS certificates/copies **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.*	No requirement to retain*
Confirmation of DBS outcome and any associated docs (e.g. risk assessment or certificate of good conduct) *Recommended within the DFE guidance, 'Data Protection: a toolkit for schools', February 2023*	Termination + 25 years
Barred list clearance *Recommended within the DFE guidance, 'Data Protection: a toolkit for schools', February 2023*	Termination + 25 years
Prohibition check *Recommended within the DFE guidance, 'Data Protection: a toolkit for schools', February 2023*	Termination + 25 years
Copies of documents used for identity authentication for DBS and Asylum and Immigration Act purposes *Recommended within Home Office 'An Employers Guide to Right to Work Checks', March 2023*	Termination + 2 years
UK Border Agency Documentation (Work permit) *Recommended within Home Office 'An Employers Guide to Right to Work Checks', March 2023*	Termination + 2 years
Records relating to employees from outside of the UK e.g. visa, work permits, etc. *Recommended within Home Office 'An Employers Guide to Right to Work Checks', March 2023*	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 *Recommended within the DFE guidance, 'Data Protection: a toolkit for schools', February 2023*	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) *Statutory*
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 *Statutory*
National minimum wage records	Three years after the end of the pay reference period following the one that the records cover. *Statutory*
Wage/salary records (also overtime, bonuses, expenses)	Termination + 6 years *Statutory*
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 *Statutory*
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 *Statutory*
Additional Employee Information	
Salary assessment forms – teachers	Current year + 6 years
Appraisal information	Current year + 6 years
Staff induction including ECTs Induction *Recommended within DFE statutory guidance 'Induction for Early Career Teachers (England), April 2023*	Completion + 6 years
Working time records	Two years from date on which they were made *Statutory*

Appendix C: Personal Data Breach Procedure

1. This procedure is based on guidance on personal data breaches produced by the ICO.
2. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
3. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO 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
4. The DPO will alert the headteacher and the chair of governors
5. 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)
6. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
7. 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
8. If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
9. The 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 secure network drive.
10. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. 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. 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. 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
- As above, any decision on whether to contact individuals will be documented by the DPO.

11. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
12. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts relating to the breach
    - 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 a secure network drive.
    - The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
13. Actions to minimise the impact of data breaches
14. We will take the actions set out below to mitigate the impact of different types of data breach, 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.
15. Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:
16. Special category data (sensitive information) being disclosed via email (including safeguarding records)
17. If special category data 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
18. Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
19. If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

20. In any cases where the recall is unsuccessful, the DPO 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
21. The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
22. The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted