



Data Protection Policy

Policy holder:	R Sharpe: Deputy Headteacher
To be reviewed by policy holder:	Annually
Last reviewed by the Governing Board:	Summer 2023
Next review by the Governing Board:	Spring 2026

Contents

1. Aims	3
2. Legislation and Guidance.....	3
3. Definitions	3
4. The Data Controller	4
5. Roles and Responsibilities	5
6. Data Protection Principles	6
7. Collecting Personal Data.....	6
8. Sharing Personal Data.....	10
9. Subject Access Requests and Other Rights of Individuals	11
10. Parental Requests to see the Educational Record	13
11. Biometric Recognition Systems	13
12. CCTV.....	14
13. Photographs and Videos.....	14
14. Data Protection by Design and Default	15
15. Data Security and Storage of Records	16
16. Disposal of Records	17
17. Personal Data Breaches.....	17
18. Training.....	17
19. Monitoring Arrangements.....	18
20. Links with Other Policies.....	18
Appendix 1: Personal Data Breach Procedure	19
Appendix 2: Privacy notice for pupils.....	18
Appendix 3: Privacy notice for parents and carers.....	23
Appendix 4: Privacy notice for the school workforce	31

Appendix 5: Privacy notice for visitors	36
---	----

Appendix 6: Retention schedule.....	
-------------------------------------	--

.....

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 the UK General Data Protection Regulation (UK GDPR) and the provisions of 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 provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the [UK GDPR](#) and the ICO’s [code of practice for subject access requests](#). It also reflects the ICO’s [code of practice](#) for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual.</p> <p>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 • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
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 as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

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.

5.1 Governing Board

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

5.2 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 SLA.

Our DPO is SchoolPro TLC Limited and is contactable via DPO@schoolpro.uk (SchoolPro TLC)

5.3 Headteacher

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

5.4 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

6. Data Protection Principles

The UK 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

7.1 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, as a public authority, can perform a **public task**, and carry out its official functions
- 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 for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- Where the above does not apply we shall request clear **consent** from the individual (or their parent/carer when appropriate in the case of a pupil)

For further detail of which lawful basis is used for each category of data, see the relevant privacy notice.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018. This is laid out in more detail in point 7.3.

If we offer online services to pupils, such as classroom apps, we intend to rely on Public Task as a basis for processing, where this is not appropriate we will get parental consent for processing (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.

7.2 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 record retention schedule.

7.3 Our processing of special categories of personal data and criminal offence data

As part of our statutory functions, we process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special Category Data

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal Conviction Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Appropriate Policy Document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This section of our Data Protection Policy document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices.

Conditions for processing special category and criminal offence data

We process special categories of personal data under the following UK GDPR Articles:

i. Article 9(2)(a) – explicit consent

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information we receive from our pupils who require a reasonable adjustment to access our services.

ii. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the school or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences.

iii. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

An example of our processing would be using health information about a pupil or member of staff in a medical emergency.

iv. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.

Examples of our processing include processing relating to any employment tribunal or other litigation.

v. Article 9(2)(g) - reasons of substantial public interest.

As a school, we are a publicly funded body and provide a safeguarding role to young and vulnerable people. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.

Examples of our processing include the information we seek or receive as part of investigating an allegation.

- vi. Article 9(2)(j) – for archiving purposes in the public interest.

The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving.

An example of our processing is the transfers we make to the County Archives as set out in our Records Management Policy.

We process criminal offence data under Article 10 of the UK GDPR

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for the school. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. Our retention with respect to this data is documented in our retention schedules.

Description of data processed

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any union. Further information about this processing can be found in our staff privacy notice.

We process the special category data about the children in our care and other members of our community that is necessary to fulfil our obligations as a school, and for safeguarding and care. This includes information about their health and wellbeing, ethnicity, photographs and other categories of data relevant to the provision of care. Further information about this processing can be found in our pupil privacy notice.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing

Special category data

We process SC data for the following purposes in Part 1 of Schedule 1:

- Paragraph 1(1) employment, social security and social protection.

We process SC data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 6(1) and (2)(a) statutory, etc. purposes
- Paragraph 18(1) – safeguarding of children and of individuals at risk

Criminal offence data

We process criminal offence data for the following purposes in parts 1, 2 and 3 of Schedule 1:

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes
- Paragraph 12(1) – regulatory requirements relating to unlawful acts and dishonesty etc
- Paragraph 18(1) – safeguarding of children and of individuals at risk
- Paragraph 36 – Extension of conditions in part 2 of this Schedule referring to substantial public interest

8. 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 may seek consent if necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT and communication companies, education support companies, and those that provide tools for learning. 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.

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.

9. Subject Access Requests and Other Rights of Individuals

9.1 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 must be submitted in writing, either by letter, email or fax to the DPO. They 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 / Headteacher.

9.2 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 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.

9.3 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.

The UK GDPR does not prevent a data subject making a subject access request via a third party. Requests from third parties are dealt with as follows:

- In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the data subject.
- It is the third party's responsibility to provide evidence of this entitlement.

- This might be a written authority to make the request or it might be a more general power of attorney.
- If there is no evidence that the third party is authorised to act on behalf of the data subject, we are not required to respond to the SAR.
- However, if we are able to contact the data subject, we will respond to them directly to confirm whether they wish to make a SAR.

9.4 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, where consent is the basis for processing
- 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 Headteacher or DPO. If staff receive such a request, they must immediately forward it to the DPO or Headteacher.

It is important to note that the school could be reported to the Information Commissioner's Office (ICO) for failing to comply with their statutory responsibilities regarding SARs and other data protection rights of the individual, and penalties (including financial) may apply.

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 records if the child attends a maintained school.

There is no equivalent legal right to access their child's educational record if the child attends an academy or free school in England or an independent school. Our school has made the decision to grant similar access to the parents of our pupils in line with the ICO's guidance, in order to retain appropriate communication between parents and the school. This similar right will only apply as long as the pupil is aged under 16. There are certain circumstances in which this similar right will

be denied, such as if releasing the information might cause 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. This list of circumstances is not exhaustive.

11. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints or a 4 digit pin code to receive school dinners instead of paying with cash), we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it (Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18). 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 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.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [guidance](#) for the use of surveillance systems including CCTV.

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 the Headteacher.

13. Photographs and Videos

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

We will not seek consent from parents/carers for photographs and videos to be taken of their child for educational purposes for use in the classroom and school displays. We will process these images under the legal basis of Public Task.

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.

Uses may include:

- Within school on public area 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 usually accompany them with any other personal information about the child, to ensure they cannot be identified.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

14. 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 data protection impact assessments (DPIAs) 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 – see section 14.1)
- 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.

14.1 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project.

We will do a DPIA for processing that is **likely to result in a high risk** to individuals as well as any other major project which requires the processing of personal data.

It is vital that the **DPIA is completed before processing is commenced** to ensure that all risks are identified and mitigated as much as possible.

Our DPIA will:

- describe the nature, scope, context, and purposes of the processing;
- assess necessity, proportionality, and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, we will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We will consult our data protection officer (SchoolPro TLC Ltd) and, where appropriate, individuals and relevant experts. We may also need to consult with relevant processors.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

We will implement the measures we identified from the DPIA, and integrate them into our policies, procedures, and practice.

15. 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 follow the relevant school procedures and ensure all records and copies are returned to the school
- 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 online safety policy/ICT policy/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)

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

16. 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. This is with the exception of data that is retained in our school archive as described in section 15.

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.

17. Personal Data Breaches

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 1.

When appropriate, we will report the data breach to the ICO within 72 hours. 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

It is important to note that the school could be reported to the Information Commissioner's Office (ICO) for high risk data breaches and penalties (including financial) may apply.

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

This policy will be reviewed and updated **every year** and shared with the full governing board.

20. Links with Other Policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online safety policy
- ICT policy
- Acceptable use policy

Appendix 1: 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 Headteacher.
- The Headteacher will investigate the report, and determine whether a breach has occurred. To decide, the Headteacher 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
- The headteacher will seek advice from the DPO and alert the chair of governors
- The Headteacher will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the DPO and relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen based on the Headteacher investigation to advise the Headteacher further
- The DPO in conjunction with the Headteacher, 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
 - Identity 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 will notify the ICO.

- The Headteacher 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 in the Breach-Log document in electronic format.
- Where the ICO must be notified, the DPO or Headteacher will do this via the [‘report a breach’ page of the ICO website](#). As required, the report 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 School will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when they expect to have further information. The Headteacher or DPO will submit the remaining information as soon as possible
- The School 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 School will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - 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 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 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 in the Breach-Log document in electronic format.

- The DPO and headteacher will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible

Actions to Minimise the Impact of Data Breaches

An example of the actions we will take to mitigate the impact of a data breach are set out below, focusing especially on a breach 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 DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- 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
- 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
- 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

Other types of breach might include:

- Details of pupil premium children being published on the school website
- Non-anonymised pupil data or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.

Appendix 2: Privacy notice for pupils

Introduction

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.

We, Penair School, are the 'data controller' for the purposes of data protection law. Our Data Protection Lead is Mr Rob Sharpe, Deputy Head Teacher (see 'Contact us' below).

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- Your contact details
- Your characteristics, like your ethnic background, language, nationality, country of birth or any special educational needs
- Your test results
- Any additional needs you may have
- Your attendance and behaviour records
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Any information required to keep you safe
- Photographs
- CCTV images
- Biometrics (such as fingerprint etc)

We may also collect other information about you if you decide to join us on a trip or visit. This might include your parents or carers contact details, passport number or health information.

We may also hold information sent to us by other organisations, including other schools, local authorities and the Department for Education.

If you would like any further details about the information we hold on you, please contact the Data Protection Lead for your school (see 'Contact us' below).

Why we use this data

We use this data to help run the school, including to:

- Get in touch with you and your parents or carers when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing including health
- To enable use of our biometric food and library systems (not in all our schools)
- For marketing purposes including websites, prospectus and social media (when consent is given)
- To celebrate your achievement
- To comply with the law

We do not currently put your personal information through any automated decision making or profiling process. This means we do not make decisions about you using only computers without any human involvement. If this changes in the future, we will update this notice to explain the processing to you, including our right to object to it.

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)
- We have a legitimate interest

For special category data (more sensitive personal information), we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in the data protection law:

- We have obtained your explicit consent to use your information in a certain way
- We need to use your information under employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protection your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The information has already been made obviously public by you
- We need to use it to make or defend against legal claims
- We need to use it for reasons of substantial public interest as defined in legislation
- We need to use it for health or social care purposes, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need it for public health reasons, and it's used by, or under the direction of, a professional

obliged to confidentiality under law

We need to use it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the use is in the public interest

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a pupil at our schools. We may also keep it after you have left the school, where we are required to by law.

We have a record retention schedule within our Data Protection (GDPR) Policy, which sets out how long we must keep information about pupils. This is in accordance with the **IRMS-Toolkit-for-Academies-v1-2019-2** <https://bluekitetrust.org.uk/wp-content/uploads/2023/03/IRMS-Toolkit-for-Academies-v1-2019-2.pdf>

The record retention schedule is based on the Information and Records Management Society's toolkit for schools.

Who we share your information with

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share your personal data with:

- Our local authority – to meet our legal duties to share certain information such as concerns about pupils' safety and exclusions

- Government departments or agencies

- Your family and representatives

- Youth support services

- Educators and examining bodies

- Our regulator (the organisation or "watchdog" that supervises us), Ofsted

- Suppliers and service providers (including online system suppliers) – so that they can provide the services we have contracted them for our auditors

- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Further education provider / next school

Please note that trainee teachers will be treated as staff whilst they complete their placement with us and therefore have access to the same information. Trainee teachers will not include any personally identifiable data within their course work, and sign a confidentiality agreement prior to commencing their placement. If the trainee wishes to include personally identifiable data, they must seek the consent of the parent/carer and, if appropriate, pupil.

Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to our local authority and/or youth support services provider, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to your name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to you once you reach the age 16.

Once you reach the age of 16, we share certain information about you with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For details of how long we store this information and how it is disposed of, see the retention schedule in our Data Protection (GDPR) Policy <https://penair.cornwall.sch.uk/wp-content/uploads/2020/12/Penair-School-Data-Protection-Policy-June-2019-1.pdf>. This is based on <https://bluekitetrust.org.uk/wp-content/uploads/2023/03/IRMS-Toolkit-for-Academies-v1-2019-2.pdf>

For more information about services for young people, please visit our local authority website.

Department for Education (DfE)

The Department for Education (a government department) collects information about you from schools and local authorities. We are legally required to share this information. For more information, please see 'How Government uses your data' section.

Transferring data internationally

Where we share data with an organisation that is based outside the UK, we will protect your data by following data protection law.

Requesting access to your personal data

Under data protection legislation, you and your parents have the right to request access to information we hold about you. To make a request or find out more information about what rights you have concerning the information we hold on you, contact the Data Protection Lead for your school – see 'Contact us' section for details.

You also have certain rights regarding how your personal information is used and kept safe. For example:

- Say that you want to access your personal information

- Say that you don't want your personal information to be used (if there is no reason for it to be used)

- Stop it being used to send you marketing materials

- Say that you don't want it to be used for automated decisions (decisions made by a computer or machine, rather than a person)

- In some cases, have it corrected if it's inaccurate

- In some cases, have it deleted or destroyed, or restrict its use

- In some cases, be notified of a data breach

- Make a complaint to the Information Commissioner's Office

- Claim compensation if the data protection rules are broken and this harms you in some way

To exercise any of these rights, please contact us (see 'Contact us' section below).

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please let us know first.

Alternatively, you can contact our Data Protection Officer, **SchoolPro TLC** by visiting [SchoolPro TLC - Education support for schools and multi academy trusts](#)

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

Where we are processing personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of personal data, please let us know by contacting the Data Protection Lead – see the ‘contact us’ section below.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Lead:

Mr Rob Sharpe

Telephone: 01872 274737

Email: rsharpe@penair.cornwall.sch.uk

This notice is based on the [Department for Education’s model privacy notice](#) for pupils, amended to reflect the way we use data in this school.

How Government uses your data

We are legally required to share information with the Department for Education (government department) through data collections:

- to help them calculate school funding as it is based upon the numbers of children and their characteristics in each school
- to inform education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures)
- to support research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

To find out more about the NPD, go to <https://www.gov.uk/guidance/apply-for-department-for-education-dfe-personal-data>.

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit: <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: <https://www.gov.uk/government/publications/dfe-external-data-shares>

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

[https://www.gov.uk/government/organisations/departments-for-education/about/personal-information-](https://www.gov.uk/government/organisations/departments-for-education/about/personal-information)

To contact DfE: <https://www.gov.uk/contact-dfe>

Appendix 3: Privacy notice for parents and carers

Introduction

Under Data Protection law, individuals have a right to be informed about how the trust/school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about pupils¹.

We, Penair school, are the 'data controller' for the purposes of Data Protection law. Our Data Protection Lead (DPL) is Mr Rob Sharpe, Deputy Head Teacher (see 'Contact us' below).

The categories of pupil information that we process include:

- Personal identifiers (such as name, unique pupil number, contact details, contact preferences, address date of birth and identification documents)
- Characteristics (such as ethnic background, nationality, language or eligibility for free school meals)
- Assessment and attainment (such as key stage 1 and phonics results, post 16 courses enrolled for and any relevant results)
- Special educational needs (including the needs and ranking)
- Medical and administration (such as doctors' information, child health, dental health, allergies, medication and dietary requirements)
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Safeguarding information (such as court orders and professional involvement)
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- Photographs
- CCTV images captured in school
- Biometrics

We may collect additional information about your child if they decide to join us on an educational trip or visit. This might include emergency contact details, passport number or UK GHIC.

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

The above is not an exhaustive list, to access the current list of categories of information each school processes, please contact the relevant Data Protection Lead (see 'Contact us' below).

Why we collect and use pupil information

We use this data to:

- Support pupil learning
- Monitor and report on pupil attainment progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Meet the statutory duties placed upon us for DfE data collections
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Enable us to carry out educational trips/visits
- To celebrate achievement
- Comply with the law regarding data sharing
- To enable the use of our biometric food services
- For marketing purposes including websites, prospectus and social media (where consent is given)

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing pupil information are:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The following data, which we collect, is classed as special category data:

- racial or ethnic origin
- religious or philosophical beliefs

- biometric data
- data concerning health (both physical and mental)
- special educational needs
- photographs and CCTV images captured in school

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing special category information are:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

We collect pupil information via registration forms, secure admissions software and secure file transfer from previous school.

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. To comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store this data

We hold pupil data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please refer to our Data Protection (GDPR) Policy, which is stored on our website <https://penair.cornwall.sch.uk/wp-content/uploads/2020/12/Penair-School-Data-Protection-Policy-June-2019-1.pdf>

The schools' record retention schedule can be found within the above policy. The schedule is based on the Information and Records Management Society's toolkit for schools.

Who we share pupil information with

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with Data Protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as pupil data, safeguarding concerns and exclusions
- Government departments and agencies
- The pupil's family and representatives
- Educators and examining bodies
- Our regulator, Ofsted
- Suppliers and service providers (including online system suppliers) – to enable them to provide the service we have contracted them for our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Further education provider/next school

Please note that trainee teachers will be treated as staff whilst they complete their placement with us and therefore have access to the same information. Trainee teachers will not include any personally identifiable data within their course work, and sign a confidentiality agreement prior to commencing their placement. If the trainee wishes to include personally identifiable data, they must seek the consent of the parent/carer and, if appropriate, pupil.

Youth support services

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16.

When carrying out data transfers to the youth support service, the data is transferred via secure method and stored as per our policy. For details of the retention period, see retention schedule in our Data Protection (GDPR) Policy <https://penair.cornwall.sch.uk/wp-content/uploads/2020/12/Penair-School-Data-Protection-Policy-June-2019-1.pdf>.

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

When carrying out data transfers to the youth support service, the data is transferred via secure method and stored as per our policy. For details of the retention period, see retention schedule in our Data Protection (GDPR) Policy <https://penair.cornwall.sch.uk/wp-content/uploads/2020/12/Penair-School-Data-Protection-Policy-June-2019-1.pdf>.

For more information about services for young people, please visit our local authority website.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under: School census - regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Transferring data internationally

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with Data Protection law.

Requesting access to your child's personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your child's personal information, or be given access to your child's educational record, contact the Data Protection Lead – see 'Contact us' section for details.

Once your child is able to understand their rights over their own data (generally considered to be over the age of 12, but this has to be considered on a case-by-case basis), we need to obtain consent from your child for you to make a subject access request on their behalf.

Please note it may be necessary for us to apply the GDPR exemption to not supply information relating to the safeguarding of a pupil if we feel that the right of access would be likely to cause serious harm to the physical or mental health of any individual.

You also have the right to:

- to ask us for access to the information we hold
- to have personal data rectified, if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- to restrict our processing of personal data (i.e. permitting its storage but no further processing)
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to our Data Protection Officer, **SchoolPro TLC** by visiting:

- [SchoolPro TLC - Education support for schools and multi academy trusts](#)

Call 0203 2909093

Or write to: SchoolPro, Harper Sheldon, Midway House, Herrick Way, Staverton Technology Park, Staverton, Cheltenham, Gloucestershire, United Kingdom, GL51 6TQ

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

Where we are processing personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of personal data, please let us know by contacting the Data Protection Lead – see the 'contact us' section.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Lead:

Mr Rob Sharpe

Telephone: 01872 274737,

Email: rsharpe@penair.cornwall.sch.uk

This notice is based on the [Department for Education's model privacy notice](#) for pupils, amended for parents and to reflect the way we use data in this school.

How Government uses your child's data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.

- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).

- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) visit:

<https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, visit: <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit: <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>.

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: [DfE external data shares - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/publications/dfes-external-data-shares)

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to

for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

<https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter>

Contact the Department for Education at <https://www.gov.uk/contact-dfe>

Appendix 4: Privacy notice for the school workforce

Introduction

Under UK data protection law, individuals have a right to be informed about how our school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **individuals we employ, or who otherwise engage to work at our school**.

Our trust, Penair school, is the 'data controller' for the purposes of UK data protection law.

Our data protection Lead (DPL) is Mr Rob Sharpe, Deputy Head Teacher (see 'Contact us' below).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about any health conditions you have that we need to be aware of
- Sickness records
- Photographs and CCTV images captured in school
- Information about trade union membership

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Why we collect and use workforce information

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body
- To enable the use of or biometric food services
- For marketing purposes including website, prospectus and social media

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing personal information for general purposes are:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing special category information are:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting workforce information

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals

Storing workforce information

We keep personal information about you while you work at our school. We may also keep it beyond your employment at our school if this is necessary. Our Data Protection Policy sets out how long we keep information about staff.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we share workforce information with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with UK data protection law), we may share personal information about you with:

- Our local authority, to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Government departments or agencies
- Our regulator, Ofsted – for inspection purposes for meeting our legal obligations
- Suppliers and service providers (including online providers) – to enable them to provide the service we have contracted them for, such as payroll, HR, pensions and banking services.
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts or tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the [government security policy framework](#).

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Data Protection Lead for the school – see ‘Contact us’ section.

You also have the right to:

- ask us for access to information about you that we hold
- have your personal data rectified, if it is inaccurate or incomplete
- request the deletion or removal of personal data where there is no compelling reason for its continued processing
- restrict our processing of your personal data (i.e. permitting its storage but no further processing)
- object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- object to decisions being taken by automated means where it produces a legal or similarly significant effect on you
- a right to seek redress, either through the ICO, or through the courts

You have a right to make a ‘subject access request’ to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances. If you would like to make a request, please contact us (see ‘Contact us’ below).

Complaints

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to our Data Protection Officer, **SchoolPro TLC** by visiting:

- [SchoolPro TLC - Education support for schools and multi academy trusts](#)
- Call 0203 2909093
- Or write to: SchoolPro, Harper Sheldon, Midway House, Herrick Way, Staverton Technology Park, Staverton, Cheltenham, Gloucestershire, United Kingdom, GL51 6TQ

Contact us

If you have any questions or concerns, or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Lead**:

Mr Rob Sharpe

Telephone: 01872 274737

Email: rsharpe@penair.cornwall.sch.uk

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on matters related to child and family social workers
- may be used to inform the distribution of school funding
- supports 'longer term' research and monitoring of children's social care policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/guidance/childrens-social-work-workforce-census-guide-to-submitting-data>

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

To contact the department: <https://www.gov.uk/contact-dfe>

Appendix 5: Privacy notice for visitors

Introduction

Under data protection law, individuals have a right to be informed about how our Trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about visitors to all our sites.

We, Penair School, are the 'data controller' for the purposes of Data Protection law. Our Data Protection Lead is Mr Rob Sharpe, Deputy Head Teacher (see 'Contact us' below).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Name

- Contact details

- Information relating to the visit, e.g. company or organisation name, arrival and departure time, car number plate

- If a professional or regular visitor, evidence that you hold an Enhanced Disclosure and Barring Service Certificate (DBS)

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to:

- Information about any access arrangements that may be required

- Photographs for identification purposes

- CCTV images captured

We may also hold data about you that we have received from other organisations, including other schools and social services.

Why we use this data

We use the data listed above to:

- Identify you and keep you safe while on the site

- Keep pupils and staff safe

Maintain accurate records of visits to site
Provide appropriate access arrangements

Use of your personal data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation

- Carry out a task in the public interest

- Where we have a legitimate interest in processing the data, for example, the use of photographs to enable us to clearly identify you in the event of an emergency evacuation

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way

- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- We have obtained your explicit consent to use your personal data in a certain way

We need to perform or exercise an obligation or right in relation to employment, social security or social protection law

We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent

The data concerned has already been made manifestly public by you

We need to process it for the establishment, exercise or defence of legal claims

We need to process it for reasons of substantial public interest as defined in legislation

We need to process it 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

We need to process it 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

We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

We have obtained your consent to use it in a specific way

We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent

The data concerned has already been made manifestly public by you

We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights

We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

Local authorities
Government departments or agencies
Police forces, courts, tribunals

How we store this data

We keep personal information about you while you are visiting our site(s). We may also keep it beyond your visit if this is necessary. Our retention schedule can be found within our Data Protection (GDPR) Policy – this sets out how long we keep information about visitors. A copy of this is available on the school website <https://penair.cornwall.sch.uk/wp-content/uploads/2020/12/Penair-School-Data-Protection-Policy-June-2019-1.pdf>

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- Our local authority [Central Bedfordshire Council] – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Government departments or agencies
- Our regulator e.g. Ofsted
- Suppliers and service providers
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations

Professional advisers and consultants
Charities and voluntary organisations
Police forces, courts, tribunals

Transferring data internationally

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

Your rights

How to access personal information that we hold about you

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

Your other rights regarding your data

Under data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:
to ask us for access to information about you that we hold

to have your personal data rectified, if it is inaccurate or incomplete

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

to restrict our processing of your personal data (i.e. permitting its storage but no further processing)

to object to direct marketing and processing for purpose of research and statistics

to object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than a person)

To exercise any of these rights, please contact us (see 'Contact us' below).

Appendix 6: Retention schedule

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to our Data Protection Officer, **SchoolPro TLC** by visiting:

- [SchoolPro TLC - Education support for schools and multi academy trusts](#)
- Call 0203 2909093
- Or write to: SchoolPro, Harper Sheldon, Midway House, Herrick Way, Staverton Technology Park, Staverton, Cheltenham, Gloucestershire, United Kingdom, GL51 6TQ

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Lead:

Mr Rob Sharpe

Telephone: 01872 274737,

Email: rsharpe@penair.cornwall.sch.uk

1. Governance, Funding and Financial Management of the Academy Trust

Academies are governed by the Academy Trust, which will usually be a company limited by guarantee³. The Academy Trust may also be a charitable trust.

1.1 Governance of the Academy Trust					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.1.1	Governance Statement	No		Life of governance statement + 6 years	SECURE DISPOSAL
1.1.2	Articles of Association	No		Life of the Academy	
1.1.3	Memorandum of Association	No		This can be disposed of once the Academy has been incorporated	SECURE DISPOSAL
1.1.4	Memorandum of Understanding of Shared Governance among Schools	No	<i>Companies Act 2006 section 355</i>	Life of Memorandum of Understanding + 6 years	SECURE DISPOSAL
1.1.5	Constitution	No		Life of the Academy	
1.1.6	Special Resolutions to amend the Constitution	No		Life of the Academy	
1.1.7	Written Scheme of Delegation	No	<i>Companies Act 2006 section 355</i>	Life of Written Scheme of Delegation + 10 years	SECURE DISPOSAL

³ A **company limited by guarantee** does not usually have a share capital or shareholders, but instead has members who act as guarantors. The guarantors give an undertaking to contribute a nominal amount (typically very small) in the event of winding up of the **company**. In the case of an Academy, the guarantors will guarantee the sum of £10 each.

1.1 Governance of the Academy Trust

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.1.8	Directors – Appointment	No		Life of appointment + 6 years	SECURE DISPOSAL
1.1.9	Directors – Disqualification	No	Company Directors Disqualification Act 1986	Date of disqualification + 15 years	SECURE DISPOSAL
1.1.10	Directors – Termination of Office	No		Date of termination + 6 years	SECURE DISPOSAL
1.1.11	Annual Report – Trustees Report	No	<i>Companies Act 2006 section 355</i>	Date of report + 10 years	SECURE DISPOSAL
1.1.12	Annual Report and Accounts	No	<i>Companies Act 2006 section 355</i>	Date of report + 10 years	SECURE DISPOSAL
1.1.13	Annual Return	No	<i>Companies Act 2006 section 355</i>	Date of report + 10 years	SECURE DISPOSAL
1.1.14	Appointment of Trustees and Governors and Directors	Yes		Life of appointment + 6 years	SECURE DISPOSAL
1.1.15	Statement of Trustees Responsibilities	No		Life of appointment + 6 years	SECURE DISPOSAL
1.1.16	Appointment and removal of Members	No		Life of appointment + 6 years	SECURE DISPOSAL
1.1.17	Strategic Review	No		Date of the review + 6 years	SECURE DISPOSAL

1.1 Governance of the Academy Trust

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.1.18	Strategic Plan [also known as School Development Plans]	No		Life of plan + 6 years	SECURE DISPOSAL
1.1.19	Accessibility Plan	There may be if the plan refers to specific pupils	Limitation Act 1980 (Section 2)	Life of plan + 6 years	SECURE DISPOSAL

1.2 Board of Directors, Members Meetings and Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
	Board of Directors				
1.2.1	Board Meeting Minutes	Could be if the minutes refer to living individuals	Companies Act 2006 section 248	Minutes must be kept for at least 10 years from the date of the meeting	OFFER TO ARCHIVES
1.2.2	Board Decisions	Could be if the decisions refer to living individuals		Date of the meeting + a minimum of 10 years	OFFER TO ARCHIVES
1.2.3	Board Meeting: Annual Schedule of Business	No		Current year	SECURE DISPOSAL
1.2.4	Board Meeting: Procedures for conduct of meeting	No	Limitation Act 1980 (Section 2)	Date procedures superseded + 6 years	SECURE DISPOSAL
	Committees⁴				
1.2.5	Minutes relating to any committees set up by the Board of Directors	Could be if the minutes refer to living individuals		Date of the meeting + a minimum of 10 years	OFFER TO ARCHIVES
	General Members' Meeting				

⁴ The board can establish any committee and determine the constitution, membership and proceedings that will apply.

1.2 Board of Directors, Members Meetings and Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.2.6	Records relating to the management of General Members' Meetings	Could be if the minutes refer to living individuals	Companies Act 2006 section 248	Minutes must be kept for at least 10 years from the date of the meetings ⁵	OFFER TO ARCHIVES
1.2.7	Records relating to the management of the Annual General Meeting ⁶	Could be if the minutes refer to living individuals	Companies Act 2006 section 248	Minutes must be kept for at least 10 years from the date of the meeting ⁷	OFFER TO ARCHIVES
	Governors				
1.2.8	Agendas for Governing Body meetings	May be data protection issues, if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL ⁸

⁵ The signed minutes must be kept securely together with the notice and agenda for the meeting and supporting documentation provided for consideration at the meeting. Documentation is generally filed in a dedicated minute book, which is usually in the form of a loose-leaf binder to which additional pages can be easily added.

⁶ Not all Academies are required to hold an Annual General Meeting for the Members – the requirement will be stated in the Constitution.

⁷ The signed minutes must be kept securely together with the notice and agenda for the meeting and any supporting documentation provided for consideration at the meeting. Documentation is generally filed in a dedicated minute book, which is usually in the form of a loose-leaf binder to which additional pages can be easily added.

⁸ In this context, SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross-cut shredder.

1.2 Board of Directors, Members Meetings and Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.2.9	Minutes of, and papers considered at, meetings of the Governing Body and its committees	May be data protection issues, if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			Life of Academy	
	Inspection Copies ⁹			Date of meeting + 3 years	SECURE DISPOSAL
1.2.10	Reports presented to the Governing Body	May be data protection issues, if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports, then the reports should be kept for the life of the Academy	SECURE DISPOSAL or retain with the signed set of minutes

⁹ These are the copies which the clerk to the Governor may wish to retain, so that requestors can view all the relevant information, without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

1.2 Board of Directors, Members Meetings and Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.2.11	Meeting papers relating to the annual parents' meeting held under Section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL
1.2.12	Trusts and Endowments managed by the Governing Body	No		PERMANENT	
1.2.13	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.2.14	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL

1.2 Board of Directors, Members Meetings and Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
	Statutory Registers¹⁰				
1.2.15	Register of Directors		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.16	Register of Directors' interests [this is not a statutory register]			Life of the Academy + 6 years	SECURE DISPOSAL
1.2.17	Register of Directors' residential addresses		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.18	Register of gifts, hospitality and entertainments		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.19	Register of members		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.20	Register of secretaries		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.21	Register of Trustees interests			Life of the Academy + 6 years	SECURE DISPOSAL
1.2.22	Declaration of Interests Statements [Governors] [this is not a statutory register]			Life of the Academy + 6 years	SECURE DISPOSAL

¹⁰ Academies are required by law to keep specific records, collectively known as statutory registers or the statutory books. The registers record information relating to the Academy's operations and structure, such as the current directors. Records should be kept up-to-date to reflect any changes that take place.

1.3 Funding and Finance					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
	Strategic Finance				
1.3.1	Statement of financial activities for the year	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.2	Financial planning	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.3	Value for money statement	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.4	Records relating to the management of VAT	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.5	Whole of government accounts returns	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.6	Borrowing powers	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.7	Budget plan	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.8	Charging and remissions policy	No		Date policy superseded + 3 years	SECURE DISPOSAL
	Audit Arrangements				
1.3.9	Audit Committee and appointment of responsible officers	No		Life of the Academy	SECURE DISPOSAL
1.3.10	Independent Auditor's report on regularity	No		Financial year report relates to + 6 years	SECURE DISPOSAL
1.3.11	Independent Auditor's report on financial statements	No		Financial year report relates to + 6 years	SECURE DISPOSAL

1.3 Funding and Finance					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
	Funding Agreements				
1.3.12	Funding Agreement with Secretary of State and supplemental funding agreements ¹¹	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.13	Funding Agreement – Termination of the funding agreement ¹²			Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.14	Funding Records – Capital Grant	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.15	Funding Records – Earmarked Annual Grant (EAG)	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.16	Funding Records – General Annual Grant (GAG)	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.17	Per pupil funding records	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.18	Exclusions agreement ¹³	No		Date of last payment of funding + 6 years	SECURE DISPOSAL

¹¹ Where there is multi-Academy governance.

¹² Either party may give not less than 7 financial years' written notice to terminate the Agreement, such notice to expire on 31 August. Or, where the Academy has significant financial issues or is insolvent, the Agreement can be terminated by the Secretary of State to take effect on the date of the notice.

¹³ The Academy can enter into an arrangement with a Local Authority (LA), so that payment will flow between the Academy and the LA, in the same way as it would do were the Academy a maintained school.

1.3 Funding and Finance					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.19	Funding records ¹⁴	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.20	Gift Aid and Tax Relief	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.21	Records relating to loans	No		Date of last payment on loan + 6 years if the loan is under £10,000 or date of last payment on loan + 12 years if the loan is over £10,000	SECURE DISPOSAL
	Payroll and Pensions				
1.3.22	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL

¹⁴ Funding agreement which says that the Academy can receive donations and can only charge where the law allows maintained schools to charge [see Charging and Remission Policy].

1.3 Funding and Finance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.23	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Regulation 15 Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)	From the end of the year in which the accounts were signed for a minimum of 6 years	SECURE DISPOSAL
1.3.24	Management of the Teachers' Pension Scheme	Yes		Date of last payment on the pension + 6 years	SECURE DISPOSAL
1.3.25	Records relating to pension registrations	Yes		Date of last payment on the pension + 6 years	SECURE DISPOSAL
1.3.26	Payroll records	Yes		Date payroll run + 6 years	SECURE DISPOSAL
	Risk Management and Insurance				
1.3.27	Insurance policies	No		Date the policy expires + 6 years	SECURE DISPOSAL
1.3.28	Records relating to the settlement of insurance claims	No		Date claim settled + 6 years	SECURE DISPOSAL
1.3.29	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
	Endowment Funds and Investments				
1.3.30	Investment policies	No		Life of the investment + 6 years	SECURE DISPOSAL

1.3 Funding and Finance					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.31	Management of Endowment Funds	No		Life of the fund + 6 years	
	Accounts and Statements				
1.3.32	Annual accounts	No		Current year + 6 years	STANDARD DISPOSAL
1.3.33	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
1.3.34	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
1.3.35	All records relating to the creation and management of budgets, including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
1.3.36	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.37	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL

1.3 Funding and Finance					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.38	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL
	Contract Management				
1.3.39	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
1.3.40	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
1.3.41	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
	Asset Management				
1.3.42	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
1.3.43	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL
1.3.44	Records relating to the leasing of shared facilities, such as sports centres	No		Current year + 6 years	SECURE DISPOSAL
1.3.45	Land and building valuations	No		Date valuation superseded + 6 years	SECURE DISPOSAL

1.3 Funding and Finance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.46	Disposal of assets	No		Date asset disposed of + 6 years	SECURE DISPOSAL
1.3.47	Community School leases for land	No		Date lease expires + 6 years	SECURE DISPOSAL
1.3.48	Commercial transfer arrangements	No		Date of transfer + 6 years	SECURE DISPOSAL
1.3.49	Transfer of land to the Academy Trust	No		Life of land ownership then transfer to new owner	SECURE DISPOSAL
1.3.50	Transfers of freehold land	No		Life of land ownership then transfer to new owner	SECURE DISPOSAL
	School Fund				
1.3.51	School Fund – Cheque books	No		Current year + 6 years	SECURE DISPOSAL
1.3.52	School Fund – Paying in books	No		Current year + 6 years	SECURE DISPOSAL
1.3.53	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
1.3.54	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
1.3.55	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
1.3.56	School Fund – Bank statements	No		Current year + 6 years	SECURE DISPOSAL

1.3 Funding and Finance					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.3.57	School Fund – Journey books	No		Current year + 6 years	SECURE DISPOSAL
	School Meals¹⁵				
1.3.58	Free school meals registers	Yes		Current year + 6 years	SECURE DISPOSAL
1.3.59	School meals registers	Yes		Current year + 3 years	SECURE DISPOSAL
1.3.60	School meals summary sheets	No		Current year + 3 years	SECURE DISPOSAL

As a charity, an Academy is not permitted to trade and make a profit. It is, however, possible to set up a subsidiary trading company, which can sell products or services and Gift Aid profits back to the Academy. If the Academy operates a subsidiary company, it is expected that these records will be managed in line with standard business practice.

1.4 Policies, Frameworks and Overarching Requirements					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.4.1	Data Protection Policy, including data protection notification	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.2	Freedom of Information Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL

¹⁵ Unless it would be unreasonable to do so, school lunches should be provided when they are requested by, or on behalf of, any pupil. A school lunch must be provided free of charge to any pupil entitled to free school lunches. From September 2014, free school lunches must be provided to all KS1 pupils.

1.4 Policies, Frameworks and Overarching Requirements					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
1.4.3	Information Security Breach Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.4	Special Educational Needs Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.5	Complaints Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.6	Risk and Control Framework	No		Life of framework + 6 years	SECURE DISPOSAL
1.4.7	Rules and Bylaws	No		Date rules or bylaws superseded + 6 years	SECURE DISPOSAL
1.4.9	Home School Agreements ¹⁶	No		Date agreement revised + 6 years	SECURE DISPOSAL
1.4.10	Equality Information and Objectives (public sector equality duty) Statement for publication	No		Date of statement + 6 years	SECURE DISPOSAL

¹⁶ This should be drawn up in consultation with parents and should apply to all pupils.

2. Human Resources

2.1 Recruitment ¹⁷					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.1.1	All records leading up to the appointment of a new Head Teacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.1.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All relevant information should be added to the Staff Personal File (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks ¹⁸	No	DBS Update Service Employer Guide June 2014	The organisation should take a copy of the DBS certificate when it is shown to them by the individual and should be added to the Staff Personal File	SECURE DISPOSAL
2.1.5	Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes		Where possible, these should be checked, and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation, then this should be added to the Staff Personal File	SECURE DISPOSAL

¹⁷ Academies do not necessarily have to employ people with qualified teacher status; only the SEN and designated LAC teacher must be qualified.

¹⁸ Academies are bound by the legislation that applies to independent schools NOT maintained schools.

2.1 Recruitment¹⁷

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom ¹⁹	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible, these documents should be added to the Staff Personal File, but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment plus not less than 2 years	SECURE DISPOSAL
2.1.7	Records relating to the employment of overseas teachers	Yes		Where possible, these documents should be added to the Staff Personal File, but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment plus not less than 2 years	SECURE DISPOSAL
2.1.8	Records relating to the TUPE process	Yes		Date last member of staff transfers or leaves the organisation + 6 years	SECURE DISPOSAL

¹⁹ Employers are required to take a “clear copy” of the documents which they are shown as part of this process.

2.2 Operational Staff Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.2.1	Staff Personal File, including employment contract and staff training records	Yes	Limitation Act 1980 (Section 2)	Termination of employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/assessment records	Yes		Current year + 5 years	SECURE DISPOSAL
2.2.4	Records relating to the agreement of pay and conditions	No		Date pay and conditions superseded + 6 years	SECURE DISPOSAL
2.2.5	Training needs analysis	No		Current year + 1 year	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes

	Basic file description	Data Protection Issues			
2.3.1	Allegation which is child protection in nature against a member of staff, including where the allegation is unfounded ²⁰	Yes	“Keeping children safe in education Statutory guidance for schools and colleges March 2015”; “Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015”	Until the person’s normal retirement age or 10 years from the date of the allegation, whichever is longer, then REVIEW	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	• Oral warning			Date of warning ²¹ + 6 months	SECURE DISPOSAL ²²
	• Written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL ²³
	• Written warning – level 2			Date of warning + 12 months	SECURE DISPOSAL ²⁴
	• Final warning			Date of warning + 18 months	SECURE DISPOSAL ²⁵

²⁰ This review took place when the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention.

²¹ Where the warning relates to child protection issues, see above. If the disciplinary proceedings relate to a child protection matter, please contact your Safeguarding Children Officer for further advice.

²² If warnings are placed on personal files, then they must be weeded from the file.

²³ If warnings are placed on personal files, then they must be weeded from the file.

²⁴ If warnings are placed on personal files, then they must be weeded from the file.

²⁵ If warnings are placed on personal files, then they must be weeded from the file.

2.3 Management of Disciplinary and Grievance Processes

	Basic file description	Data Protection Issues			
	<ul style="list-style-type: none"> Case not found 			If the incident is child protection related, then see above; otherwise, dispose of at the conclusion of the case	SECURE DISPOSAL

2.4 Health and Safety

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.4.1	Health and Safety policy statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety risk assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents, a further retention period will need to be applied	SECURE DISPOSAL

2.4 Health and Safety

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.4.4	Accident reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	The official Accident Book must be retained for 3 years after the last entry in the book. The book may be in paper or electronic format The incident reporting form may be retained as below	
	<ul style="list-style-type: none"> Adults 			Date of incident + 6 years	SECURE DISPOSAL
	<ul style="list-style-type: none"> Children 			Date of birth of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No		Current year + 10 years then REVIEW	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have come into contact with asbestos	No		Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have come into contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire precautions log books	No		Current year + 6 years	SECURE DISPOSAL
2.4.9	Fire risk assessments	No	Fire Service Order 2005	Life of the risk assessment + 6 years	SECURE DISPOSAL

2.4 Health and Safety					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
2.4.10	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL

3. Management of the Academy

3.1 Admissions					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.1.1	All records relating to the creation and implementation of the School Admissions' Policy	No	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	Yes	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

3.1 Admissions					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.1.3	Admissions – if the appeal is unsuccessful	Yes	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
3.1.4	Register of admissions	Yes	School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of 3 years after the date on which the entry was made ²⁶	REVIEW Schools may wish to consider keeping the admission register permanently, as often schools receive enquiries from past pupils to confirm the dates they attended the school
3.1.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL

²⁶ School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities October 2014 p6.

3.1 Admissions

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.1.6	Proofs of address supplied by parents as part of the admissions process	Yes	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
3.1.7	Supplementary information form, including additional information such as religion and medical conditions	Yes			
	<ul style="list-style-type: none"> For successful admissions 			This information should be added to the pupil file	SECURE DISPOSAL
	<ul style="list-style-type: none"> For unsuccessful admissions 			Until appeals process completed	SECURE DISPOSAL

3.2 Head Teacher and Senior Management Team					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.2.1	Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then REVIEW	These could be of permanent historical value and should be offered to the County Archives Service, if appropriate
3.2.2	Minutes of Senior Management Team meetings and meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then REVIEW	SECURE DISPOSAL
3.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then REVIEW	SECURE DISPOSAL
3.2.4	Records created by Head Teachers, Deputy Head Teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then REVIEW	SECURE DISPOSAL
3.2.5	Correspondence created by Head Teachers, Deputy Head Teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then REVIEW	SECURE DISPOSAL
3.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL

3.3 Operational Administration					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
3.3.1	Management of complaints	Yes		Date complaint resolved + 3 years	SECURE DISPOSAL
3.3.2	Records relating to the management of contracts with external providers	No		Date of last payment on contract + 6 years	SECURE DISPOSAL
3.3.3	Records relating to the management of software licences	No		Date licence expires + 6 years	SECURE DISPOSAL
3.3.4	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
3.3.5	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
3.3.6	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
3.3.7	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
3.3.8	Visitors' books and signing in sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
3.3.9	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
4.1.1	Title deeds of properties belonging to the school	No		These should follow the property, unless the property has been registered with the Land Registry	
4.1.2	Plans of property belonging to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold	
4.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL
4.1.5	Business continuity and disaster recovery plans	No		Date the plan superseded + 3 years	SECURE DISPOSAL

4.2 Maintenance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees, including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

4.3 Fleet Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
4.3.1	The process of acquisition and disposal of vehicles through lease or purchase, e.g., contracts/leases, quotes, approvals	N	Limitation Act 1980 (Section 2)	Disposal of the vehicle + 6 years	SECURE DISPOSAL
4.3.2	The process of managing allocation and maintenance of vehicles, e.g., lists of who was driving the vehicles and when, maintenance	N	Limitation Act 1980 (Section 2)	Disposal of the vehicle + 6 years	SECURE DISPOSAL
4.3.3	Service logs and vehicle logs	N	Limitation Act 1980 (Section 2)	Life of the vehicle, then either to be retained for 6 years by school or to be returned to lease company	SECURE DISPOSAL
4.3.4	GPS tracking data relating to the vehicles	N	Limitation Act 1980 (Section 2)	Date of journey + 6 years	SECURE DISPOSAL

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting, see under Health and Safety above.

5.1 Pupil's Educational Record					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	<ul style="list-style-type: none"> Primary 			Retain whilst the child remains at the primary school	<p>The file should follow the pupil when they leave the primary school. This will include:</p> <ul style="list-style-type: none"> To another primary school To a secondary school To a pupil referral unit <p>If the pupil dies whilst at primary school, the file should be returned to the LA to be retained for the statutory retention period.</p> <p>If the pupil transfers to an independent school, transfers to home schooling or leaves the country, the file should be returned to the LA to be retained for the statutory retention period.</p> <p>Primary schools do not ordinarily</p>

5.1 Pupil's Educational Record

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
					have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the LA, as it is more likely that the pupil will request the record from the LA
	<ul style="list-style-type: none"> Secondary 		Limitation Act 1980 (Section 2)	Date of birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Records relating to the management of exclusions	Yes		Date of birth of the pupil involved + 25 years	SECURE DISPOSAL
5.1.3	Management of examination registrations	Yes		The examination board will usually mandate how long these records need to be retained	
5.1.4	Examination results – pupil copies	Yes			
	<ul style="list-style-type: none"> Public 			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board
	<ul style="list-style-type: none"> Internal 			This information should be added to the pupil file	
	This review took place when the Independent Inquiry on Historical Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention				

5.1 Pupil's Educational Record					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
5.1.5	Child protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	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	SECURE DISPOSAL – these records MUST be shredded
5.1.6	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Date of birth 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 LA Social Services record	SECURE DISPOSAL – these records MUST be shredded

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Attendance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
5.2.1	Attendance registers	Yes	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
5.2.2	Correspondence relating to authorised absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time in order to defend themselves in a “failure to provide a sufficient education” case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period – this should be documented

5.3 Special Educational Needs					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL, unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL, unless the document is subject to a legal hold
5.3.4	Accessibility strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL, unless the document is subject to a legal hold

6. Curriculum Management

6.1 Statistics and Management Information

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination results (schools copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATs records –	Yes			
	<ul style="list-style-type: none"> Results 			<p>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</p> <p>The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison</p>	SECURE DISPOSAL
	<ul style="list-style-type: none"> Examination papers 			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value added and contextual data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self-evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
6.2.1	Schemes of work	No		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
6.2.2	Timetable	No		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
6.2.3	Class record books	No		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
6.2.4	Mark books	No		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
6.2.5	Record of homework set	No		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
6.2.6	Pupils' work	No		Where possible, 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

7. Extracurricular Activities

7.1 Educational Visits outside the Classroom

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
7.1.1	Records created by schools in order to obtain approval to run an educational visit outside the classroom – Primary schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 – "Legal Framework and Employer Systems" and Section 4 – "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools in order to obtain approval to run an educational visit outside the classroom – Secondary schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 – "Legal Framework and Employer Systems" and Section 4 – "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident ²⁷	Yes		Conclusion of the trip	Although the consent forms could be retained for date of birth + 25 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time

²⁷ One-off or blanket consent: The Department for Education (DfE) has prepared a one-off consent form to be signed by the parent on enrolment of their child in a school. This form is intended to cover all types of visits and activities where parental consent is required. The form is available on the DfE website for establishments to adopt and

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	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	
7.1.5	Records relating to residential trips	Yes		Date of birth of youngest pupil involved + 25 years	SECURE DISPOSAL

7.2 Walking Bus					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
7.2.1	Walking bus registers	Yes		Date of register + 3 years. This takes into account the fact that, if there is an incident requiring an accident report, the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]

adapt, as appropriate, at www.gov.uk/government/publications/consent-for-school-trips-and-other-off-site-activities. A similar form could be used for other establishments, such as Early Years Foundation Stage (EYFS) providers and youth groups, or at the start of programmes for young people.

8. Central Government and Local Authority (LA)

This section covers records created in the course of interaction between the school and the LA.

8.1 Local Authority					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
8.1.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School census returns	No		Current year + 5 years	SECURE DISPOSAL

8.2 Central Government					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
8.2.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL