Gillotts School

Data Protection Policy

Contents

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 (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 guidance on subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

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

	• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal information 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 Local Governing Body

The Local Governing Body of the school 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 appointed by the River Learning Trust and is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law and developing related policies and guidelines where applicable.

The DPO is also the point of contact for the ICO.

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

Our DPO is Louise Askew, Head of Governance and Compliance at River Learning Trust, and is contactable via laskew@riverlearningtrust.org.

5.3 Data Protection Lead

The Data Protection Lead (DPL) is the staff member in our school responsible for overseeing the implementation of this policy and monitoring compliance with data protection law in the school. The DPL is the first point of contact for individuals whose data the school processes.

Our DPL is Catharine Darnton, Headteacher and is contactable via cdarnton@gillotts.org.

5.4 Headteacher

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

5.5 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 DPL 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.

Where applicable, the DPL will seek advice and guidance from the DPO.

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

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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 records management policy.

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 will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

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

When 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.

An individual can make a Subject Access Request verbally or in writing (letter and email), including by social media.

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 inform the DPL. The DPL will then immediately inform the DPO and seek advice and guidance before taking any action.

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 aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

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.

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;
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Challenge processing which has been justified on the basis of public interest;
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area;
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);

- Prevent processing that is likely to cause damage or distress;
- Be notified of a data breach in certain circumstances;
- Make a complaint to the ICO;
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

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

10. Parental requests to see the educational record

As our school is an academy, parents, or those with parental responsibility, do not have an automatic parental right to free access to their child's educational record (which includes most information about a pupil). The school will decide on a case-by-case basis whether to grant such requests, bearing in mind guidance issued from time to time from the Information Commissioner's Office.

The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

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

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, a cashless catering system), 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. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

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 code of practice for the use of 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 Karen Barker, Business Manager, kbarker@gillotts.org..

13. Photographs and videos

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

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Permitted uses may include:

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

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

Written consent will also be obtained from staff members before photographs and videos of them are used for the above purposes.

See our Child Protection Policy and Online Safety 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 suitable DPL, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6);
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPL and the Trust's 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

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 securely 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;
- Password complexity is forced for all members of the Trust and reuse of passwords is not permitted. The minimum password length is 8, increasing to 12 for more sensitive accounts. All staff and governors accounts are protected by 2 step verification. All accounts are protected by context aware access that prohibits access outside of the UK without express permissions being granted;
- 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 Acceptable Use Policy and Staff Handbook);
- 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).

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.

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.

18. Training

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

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

19. Monitoring arrangements

The DPL is responsible for monitoring the implementation of this policy in school.

This policy will be reviewed **every 2 years** and shared with the local governing body.

20. Links with other policies

This data protection policy should be read in conjunction with the following Trust policies:

- Records Management Policy
- Staff IT Acceptable Use Policy

Date adopted: 4 March 2025
Next review: Spring 2027 (thereafter review every two years)

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 DPL who will then inform the DPO who will offer help and guidance in dealing with the breach.
- The DPL will investigate the report and determine whether a breach has occurred. To decide, the DPL 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 DPL will alert the headteacher and the chair of governors.
- The DPL will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPL and DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPL and DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPL and DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned.

  If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned;
        - The categories and approximate number of personal data records concerned.

    - The name and contact details of the DPO;
    - A description of the likely consequences of the personal data breach;
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - 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 DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPL 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).

  All breaches will be recorded in the school's GDPR drive.
- In the case of a breach that is reportable to the ICO, the DPO, DPL and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

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

The following sets out examples of the relevant actions we will take for different types of risky or sensitive personal data processed by the school. For example:

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 DPL as soon as they become aware of the error.*
- *If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the IT Services to recall it.*
- *In any cases where the recall is unsuccessful, the DPL 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 DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.*
- *The DPL 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*

Sensitive information being disclosed on the school website

- *If special category data (sensitive information) is accidentally made available on the website, the publisher must remove it as soon as they become aware of the error.*
- *If members of staff, see the data they must alert the publisher and the DPL as soon as they become aware of the error*
- *If the publisher is not available or cannot remove it for any reason, the DPL will ask the IT Services to remove it.*

Non-anonymised pupil data or staff pay information being shared with governors

- *If special category data (sensitive information) is accidentally made available via email to governors, the sender must attempt to recall the email as soon as they become aware of the error.*
- *Governors who receive personal data sent in error must alert the sender and the DPL as soon as they become aware of the error.*
- *If the sender is unavailable or cannot recall the email for any reason, the DPL will ask IT Services to recall it.*
- *In any cases where the recall is unsuccessful, the DPL will contact the relevant governors 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 DPL will ensure we receive a written response from all the governors who received the data, confirming that they have complied with this request.*
- *If special category data (sensitive information) is accidentally made available via paper to governors, the sender must request all governors return the information so that it can be shredded. The sender will ensure she/he receives a written response from all the governors who received the data, confirming that they have complied with this request.*

Appendix 2: Privacy Notice (How we use pupil information)

The categories of pupil information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- 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)
- assessment and attainment (such as post 16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- trips and activities
- catering and free school meal management
- identity management/authentication
- data about use of the school's IT systems

This list is not exhaustive.

Why we collect and use pupil information

We collect and use pupil information, for the following purposes:

- to support pupil learning
- to monitor and report on pupil attainment and progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to keep children safe (food allergies, or emergency contact details)
- to enable pupils to purchase food
- to meet the statutory duties placed upon us for the Department for Education (DfE) data collections
- to promote the school on our school website, display boards and other printed publications to parents and the wider community

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

For the purposes of:

- to support pupil learning
- to monitor and report on pupil attainment progress
- to provide appropriate pastoral care
- to assess the quality of our services

in accordance with the 'public task' basis – we need to process data to fulfil our official duties as a school.

For the purposes of:

- to meet the statutory duties placed upon us by the Department for Education
- to support NHS school immunisation programme

in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law.

For the purposes of:

- to promote the school on our school website, display boards and other printed publications to parents and the wider community
- to allow students to purchase food

in accordance with the 'consent' basis – we will obtain consent from you to use your personal data.

For the purposes of:

- to keep children safe (food allergies, or emergency contact details)

in accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation.

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 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. protect 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 to use 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.

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 obviously public by you.
- We need to use it as part of legal proceedings, to obtain legal advice, or to make or defend against legal claims.
- We need to use it for reasons of substantial public interest as defined in legislation.

Collecting pupil information

We collect pupil information via the Student Information Form, on admission, and through the Common Transfer File (CTF) from the 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. In order 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.

Storing pupil 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 see our Data Protection Policy.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our multi-academy trust, River Learning Trust
- our local authority, Oxfordshire
- youth support services (pupils aged 13+)

- our school nurse and school counsellors
- awarding bodies
- the NHS, in relation to the schools immunisation programme
- the Department for Education (DfE)

We also provide pupil level personal data to third party organisations which supply services to us for which the provision of the data is essential for the service to be provided. Decisions on whether to release this data are subject to a robust approval process, including the arrangements in place to store and handle the data. We currently provide pupil level data for the following purposes:

- Systems integral to the delivery of core business services, e.g. SIMS, Edulink, SISRA, Schoolcomms
- Systems integral to the operation of IT Services systems, e.g. Google, EE, Salamander
- Curriculum products, e.g. ExamPro, Sparx Maths, ActiveLearn

A full current list is available on request.

Why we regularly share pupil information

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

Youth support services

Pupils aged 13+

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.

Data is securely transferred to the youth support service via secure email.

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

Department for Education (DfE)

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 regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by the Department for Education (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. For privacy information on the data the Department for Education collects and uses, please see:
https://www.gov.uk/government/publications/privacy-information-early-years-foundation-stage-to-key-stage-3

and

https://www.gov.uk/government/publications/privacy-information-key-stage-4-and-5-and-adult-education

Requesting access to your personal data

The UK-GDPR gives parents and pupils certain rights about how their information is collected and used. To make a request for your personal information, or be given access to your child's educational record, contact Leanne Herbert, PA to the Headteacher, lherbert@gillotts.org.uk.

You also have the following rights:

- the right to be informed about the collection and use of your personal data – this is called 'right to be informed'.
- the right to ask us for copies of your personal information we have about you – this is called 'right of access', this is also known as a subject access request (SAR), data subject access request or right of access request.
- the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification'.
- the right to ask us to delete your personal information – this is called 'right to erasure'
- the right to ask us to stop using your information – this is called 'right to restriction of processing'.
- the 'right to object to processing' of your information, in certain circumstances
- rights in relation to automated decision making and profiling.
- the right to withdraw consent at any time (where relevant).
- the right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. For example, some rights will not apply:

- right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent.

If you have a concern 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 the Information Commissioner's Office at raise a concern with ICO.

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 your 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 your personal data, please let us know by contacting Leanne Herbert, PA to the Headteacher, lherbert@gillotts.org.uk.

Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated on 4 March 2025.

Contact

If you would like to discuss anything in this privacy notice, please contact: Leanne Herbert, PA to the Headteacher, lherbert@gillotts.org.uk.

How Government uses your data

The pupil data that we lawfully share with the Department for Education (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 (DfE) (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education (DfE) and contains information about pupils in schools in England. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

The data in the NPD is provided as part of the operation of the education system and is used for research and statistical purposes to improve, and promote, the education and well-being of children in England.

The evidence and data provide DfE, education providers, Parliament and the wider public with a clear picture of how the education and children's services sectors are working in order to better target, and evaluate, policy interventions to help ensure all children are kept safe from harm and receive the best possible education.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-npd-privacy-notice/national-pupil-database-npd-privacy-notice

Sharing by the Department for Education (DfE)

DfE will only share pupils' personal data where it is lawful, secure and ethical to do so. Where these conditions are met, the law allows the Department for Education (DfE) to share pupils' personal data with certain third parties, including:

- schools and 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 for Education's (DfE) NPD data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact the Department for Education (DfE) to request access to individual level information relevant to detecting that crime.

For information about which organisations the Department for Education (DfE) 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

How to find out what personal information the Department for Education (DfE) holds about you

Under the terms of the UK GDPR, you are entitled to ask the Department for Education (DfE):

- 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 for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

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

or

https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights

To contact the Department for Education (DfE): https://www.gov.uk/contact-dfe

Appendix 3: Privacy Notice (How we use workforce information)

The categories of school information that we process

These include:

- personal information (such as name, employee or teacher number, national insurance number, address, phone number; next of kin and emergency contact numbers)
- characteristics information (such as, sex, age, ethnic group and, where relevant, medical information)
- contract information (such as start date, hours worked, post, roles, salary, pension)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- performance information (such as appraisals, lesson observations, marking reviews, CPD records)
- outcomes of formal procedures (such as disciplinary, grievance)
- biometric data
- photographs
- CCTV footage
- data about your use of the school's IT systems

This list is not exhaustive.

Why we collect and use workforce information

We use workforce data to:

- enable individuals to be paid
- facilitate safe recruitment
- support effective performance management
- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- allow better financial modelling and planning
- enable ethnicity and disability monitoring
- to meet the statutory duties placed upon us by the Department for Education
- to promote the school on our school website, display boards and other printed publications to parents and the wider community
- enable staff to purchase food

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

For the purposes of:

- facilitate safe recruitment
- support effective performance management
- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- allow better financial modelling and planning
- enable ethnicity and disability monitoring

in accordance with the 'public task' basis – we need to process data to fulfil our official duties as a school.

For the purposes of:

- to meet the statutory duties placed upon us by the Department for Education

in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law.

For the purposes of:

- enable individuals to be paid

in accordance with the 'fulfil a contract' basis - we need to process data to meet our contractual obligations to you.

For the purposes of:

- to promote the school on our school website, display boards and other printed publications to parents and the wider community
- to allow students to purchase food

in accordance with the 'consent' basis – we will obtain consent from you to use your personal data.

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 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. protect 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 to use 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.

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 obviously public by you.
- We need to use it as part of legal proceedings, to obtain legal advice, or to make or defend against legal claims.
- We need to use it for reasons of substantial public interest as defined in legislation.

Collecting workforce information

We collect personal information via our new starter's forms.

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with UK GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold 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 please see our Data Protection Policy.

Who we share workforce information with

We routinely share this information with:

- our multi-academy trust, River Learning Trust

- our local authority, Oxfordshire
- the Department for Education (DfE)

We also provide staff level personal data to third party organisations which supply services to us for which the provision of the data is essential for the service to be provided. Decisions on whether to release this data are subject to a robust approval process, including the arrangements in place to store and handle the data. We currently provide staff level data for the following purposes:

- Systems integral to the delivery of core business services, e.g. SIMS, Edulink, SISRA, Schoolcomms
- Systems integral to the operation of IT Services systems, e.g. Google, EE, Salamander
- Curriculum products, e.g. ExamPro, Sparx Maths, ActiveLearn

A full current list is available on request.

Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

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 school employees with the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by the Department for Education (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.

For privacy information on the data the Department for Education (DfE) collects and uses, please see: https://www.gov.uk/government/publications/privacy-information-education-providers-workforce-including-teachers.

Requesting access to your personal data

The UK-GDPR gives you certain rights about how your information is collected and used. To make a request for your personal information, contact: Leanne Herbert, PA to the Headteacher, lherbert@gillotts.org.uk.

You also have the following rights:

- the right to be informed about the collection and use of your personal data – this is called 'right to be informed'.
- the right to ask us for copies of personal information we have about you – this is called 'right of access', this is also known as a subject access request, data subject access request or right of access request.
- the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification'.
- the right to ask us to delete your personal information – this is called 'right to erasure'
- the right to ask us to stop using your information – this is called 'right to restriction of processing'.
- the 'right to object to processing' of your information, in certain circumstances
- rights in relation to automated decision making and profiling.
- the right to withdraw consent at any time (where relevant).
- the right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. For example, some rights will not apply:

- right to erasure does not apply when the lawful basis for processing is a legal obligation or public task.
- right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent.

If you have a concern 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 the Information Commissioner's Office at raise a concern with ICO.

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 your 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 your personal data, please let us know by contacting Leanne Herbert, PA to the Headteacher, lherbert@gillotts.org.uk.

Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated on 4 March 2025.

Contact

If you would like to discuss anything in this privacy notice, please contact: Leanne Herbert, PA to the Headteacher, lherbert@gillotts.org.uk.

How Government uses your data

The workforce data that we lawfully share with the Department for Education (DfE) through data collections:

- informs the Department for Education (DfE) policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (DfE) including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department for Education (DfE)

The Department for Education (DfE) 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 for Education (DfE) will only share your personal data where it is lawful, secure and ethical to do so and 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 the Department for Education (DfE) releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of public benefit, proportionality, legal underpinning and strict information security standards.

For more information about the Department for Education's (DfE) data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the Department for Education (DfE) has provided information, (and for which project) please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

How to find out what personal information the Department for Education (DfE) hold about you

Under the terms of UK GDPR, you're entitled to ask the Department for Education (DfE):

- 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 for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

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

or

https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights

To contact the Department for Education (DfE): https://www.gov.uk/contact-dfe

Appendix 4: Privacy Notice (How we use school governor information)

The categories of governance information that we process include:

- personal identifiers, contacts and characteristics (such as name, date of birth, contact details, address and postcode)
- governance details (such as role, start and end dates)
- information about business and pecuniary interests

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 governance information

The personal data collected is essential, in order for the school, academy or academy trust to fulfil their official functions and meet legal requirements.

We collect and use governance information, for the following purposes:

a) establish and maintain effective governance

b) meet statutory duties for publishing and sharing governors' details

c) facilitate safe recruitment, as part of our safeguarding obligations towards pupils

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

- for the purpose **a)** named above in accordance with the legal basis of **Public Task**
- for the purpose **b)** and **c)** named above in accordance with the legal basis of **Legal Obligation**

All local authority maintained school governing bodies, under section 538 of the Education Act 1996, and academy trusts, under the academy trust handbook, have a legal duty to provide the governance information as detailed above.

Collecting governance information

We collect personal information via governor contact forms, declarations of interest and through viewing your DBS certificate.

Governance roles data is essential for the school and academy trust's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it may be requested on a voluntary basis. In order to comply with UK-GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing governance information

We hold 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 please see our Data Protection Policy.

Who we share governance information with

We routinely share this information with:

- our multi-academy trust, River Learning Trust
- our local authority, Oxfordshire
- the Department for Education (DfE)

Why we share governance information

We do not share information about individuals in governance roles with anyone without consent unless the law and our policies allow us to do so.

The Department for Education (DfE) collects personal data from educational providers and local authorities. We are required to share information about individuals in governance roles with the Department for Education (DfE) under the requirements set out in the academy trust handbook.

All data is entered manually on the GIAS service and held by the Department for Education (DfE) under a combination of software and hardware controls which meet the current government security policy framework.

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

Requesting access to your personal data

The UK GDPR gives you certain rights about how your information is collected and used. To make a request for your personal information, contact Leanne Herbert, PA to the Headteacher, lherbert@gillotts.org.uk.

Your rights include:

- the right to be informed about the collection and use of your personal data – this is called 'right to be informed'.
- the right to ask us for copies of personal information we have about you – this is called 'right of access', this is also known as a subject access request (SAR), data subject access request or right of access request.
- the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification'.
- the right to ask us to delete your personal information – this is called 'right to erasure'.
- the right to ask us to stop using your information – this is called 'right to restriction of processing'.
- the 'right to object to processing' of your information, in certain circumstances.
- rights in relation to automated decision making and profiling.
- the right to withdraw consent at any time (where relevant).
- the right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why your information rights request may be refused. For example, some rights will not apply:

- right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't have the right to object, but you have the right to withdraw consent.

If you have a concern 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 the Information Commissioner's Office at raise a concern with ICO.

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 your 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 your personal data, please let us know by contacting Leanne Herbert, PA to the Headteacher, lherbert@gillotts.org.uk.

Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated on 4 March 2025.

Contact

If you would like to discuss anything in this privacy notice, please contact: Leanne Herbert, PA to the Headteacher, lherbert@gillotts.org.uk.

How government uses your data

The governance data that we lawfully share with the Department for Education (DfE) via GIAS will:

- increase the transparency of governance arrangements
- enable local authority maintained schools, academies, academy trusts and the Department for Education (DfE) to identify more quickly and accurately individuals who are involved in governance and who govern in more than one context
- allow the Department for Education (DfE) to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role

Data collection requirements

To find out more about the requirements placed on us by the Department for Education (DfE) including the data that we share with them, go to https://www.gov.uk/government/news/national-database-of-governors

Some of these personal data items are not publicly available and are encrypted within the GIAS system. Access is restricted to authorised Department for Education (DfE) and education establishment users with a Department for Education (DfE) Sign-in (DSI) account who need to see it in order to fulfil their official duties. The information is for internal purposes only and not shared beyond the Department for Education (DfE) unless the law allows it.

How to find out what personal information the Department for Education (DfE) hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department for Education (DfE):

- 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 for Education (DfE), you should make a subject access request (SAR). Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

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

or

https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights

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

Appendix 5: Retention Schedule

Pupil records

Document type	Retention period	Action at end of retention period	Further information
Secondary school pupil records	Until the pupil's 25th birthday.	Dispose of records securely. If the pupil leaves to go to another school, transfer the records to that school. There is guidance on what to do if the school closes before the end of the retention period.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the education record. Retain as detailed in section 2 of the Limitation Act 1980.
Special educational needs and disabilities (SEND), including SEND statements and accessibility plans	Until the pupil's 30th birthday.	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.	SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980.
Attendance and absence	Until the pupil's 30th birthday.	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.	SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980.

Child protection records

Document type	Retention period	Action at end of retention period	Further information
Child protection files	Until the child's 25th birthday. If the file relates to child sexual abuse, retain until the child's 75th birthday.	Dispose of records securely. Child protection files should be passed on to any new school a child attends. This should be transferred separately from the main pupil file.	Should be stored in a separate child protection file. Keeping children safe in education sections 66, 67, 121 and 122. The Report of the Independent Inquiry into Child Sexual Abuse (IICSA), recommendation on access to records.
Allegations of child protection against a member of staff, including unfounded allegations	Until the staff member's normal retirement age, or 10 years from the date of the allegation, whichever is later.	Dispose of records securely.	Keeping children safe in education. Working together to safeguard children.

Finance records

Document type	Retention period	Action at end of retention period	Further information
Contracts	6 years from the last payment on the contract.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Debtor's records	6 years from the end of the financial year.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
VAT records	6 years from the end of the financial year.	Dispose of records securely.	May include invoices, budgets, bank statements and annual accounts. Record keeping (VAT Notice 700/21).

Governance records

Document type	Retention period	Action at end of retention period	Further information
Admissions	3 years from the admission date.	Dispose of records securely.	Working together to improve school attendance.
Attendance registers	3 years from the date of entry.	Dispose of records securely.	Regulation 14 of the Education (Pupil Registration) (England) Regulations 2006.
Annual governors report	10 years.	Dispose of records securely.	The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002. Retain as detailed in section 2 of the Limitation Act 1980.
Curricular record	At least one year.	Dispose of records securely.	The Education (School Records) Regulations 1989. Regulation 3 of the Education (Pupil Information) (England) Regulations 2005.
Directors – disqualification	15 years from the date of disqualification.	Dispose of records securely.	The Education (Company Directors Disqualification Act 1986: Amendments to Disqualification Provisions) (England) Regulations 2004
Records of educational visits	10 years from the date of the visit. If there was an incident on the visit, retain the permission slips for all pupils and the incident report in the pupil record, or until the pupil reaches the age of 25.	Dispose of records securely.	Health and safety on educational visits. Retain as detailed in section 2 of the Limitation Act 1980.

Document type	Retention period	Action at end of retention period	Further information
School vehicles	6 years from the disposal of the vehicle.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Statutory registers and compliance	Retention periods vary, for example: Memorandums of understanding should be retained for the life of the academy plus 6 years. Annual reports should be retained for 10 years from the date of the report. Board meeting records should be retained for 10 years from the date of the meeting.	Dispose of records securely.	May include annual reports and governance records. Companies Act 2006 contains information on which statutory registers to keep. Compliance guidance in the maintained schools governance guide. Compliance guidance in the academy trust governance guide. Academy trust handbook.

Health and safety records

Document type	Retention period	Action at end of retention period	Further information
Accessibility plans	Life of plan plus 6 years.	Dispose of records securely.	Retain as detailed in section 2 of the Limitation Act 1980.
Accident records	3 years from the date of the accident.	Dispose of records securely.	Accidents involving pupils should be retained in the pupil record. Regulation 25 of the Social Security (Claims and Payments) Regulations 1979.
Monitoring exposure to substances hazardous to health, including asbestos	5 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002.
Health surveillance records	40 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. Health surveillance - Record keeping.
Other health records of staff	While the worker is employed in your school.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. Health surveillance - Record keeping.
Fire assessments	Life of the risk assessment plus 6 years.	Dispose of records securely.	Fire Service Order 2005. Retain as detailed in section 2 of the Limitation Act 1980.

Property records

Document type	Retention period	Action at end of retention period	Further information
Maintenance records	6 years from the end of the financial year.	Dispose of records securely.	Record keeping (VAT Notice 700/21).
Title deeds	12 years from the end of the deed.	Dispose of records securely.	Section 2 of the Limitation Act 1980.

Staff records

Document type	Retention period	Action at end of retention period	Further information
Copies of DBS certificates	6 months from the date of recruitment.	Dispose of records securely.	Keeping children safe in education.
Maternity pay records	3 years after the end of the tax year in which the maternity pay period ends.	Dispose of records securely.	The Statutory Maternity Pay (General) Regulations 1986.
Pay records	3 years from the end of the tax year they relate to.	Dispose of records securely.	PAYE and payroll for employers: Keeping records.
Personnel files	6 years from termination of employment.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Retirement benefits	A minimum of 6 years from the end of the year in which the accounts were signed.	Dispose of records securely.	Regulation 15 of the Retirement Benefits Schemes (Information Powers) Regulations 1995.