# Data Protection Policy

The King's School
Cadhay Lane
Ottery-St-Mary
Devon
EX11 1RA

## Policy Change Control

| | |
|---|---|
| Policy Owner | Director of Finance & Operations |
| Approved By | Resources Committee |
| Date of Last Approval | 27/06/2024 |
| Next Revision Due | May 2026 |

| Date | Version | Person | Change / Action |
|---|---|---|---|
| 09/04/2018 | 1.0 | SBM | Initial Draft of Policy |
| 09/05/2018 | 1.0 | Trustees | Approved by Trustees Resources Committee |
| 10/06/2019 | 1.1 | SBM | Review – No substantive changes. |
| 19/06/2019 | 1.1 | Trustees | Approval |
| 17/04/2020 | 1.1 | SBM | Review – No substantive changes |
| 24/06/2020 | 1.2 | Trustees | Approval following minor changes |
| 17/05/2021 | 1.3 | SBM | A few minor updates |
| 23/06/2021 | 1.3 | Trustees | Approval |
| 20/06/2022 | 1.4 | SBM | A few minor updates and the addition of the Local Authority as an organisation we share data with |
| 29/06/2022 | 1.4 | Trustees | Approval |
| 19/06/2023 | 1.5 | DFO | Update to change SBM to DFO and updated to include references to the DFO |
| 28/06/2023 | 1.5 | Trustees | Approved |
| 22/04/2024 | 1.6 | DFO | Inclusion of DPIAs information (S.14.1) and other minor updates |
| 26/07/2024 | 1.6 | Trustees | Approved |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 1. Aims

1.1 The King's School aims to ensure that all personal data collected about staff, students, parents, trustees, 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).

1.2 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## 2. Legislation and guidance

2.1 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.

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

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

2.4 In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 (as amended in 2018), which gives parents the right of access to their child's educational record as well as complying with our funding agreement and articles of association.

2.5

This policy should be read in conjunction with the following policies and documents:

- Safeguarding (Child Protection) Policy
- DBS Disclosure Policy
- Privacy Notice – Parents and Carers
- Privacy Notice – Students
- Privacy Notice – Staff and Volunteers
- Freedom of Information Act Policy and Publication Scheme

## 3. Definitions

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials) |

| | |
|---|---|
| | • Identification number<br>• Location data<br>• Online identifier, such as a username<br>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:<br>• Racial or ethnic origin<br>• Political opinions<br>• Principles<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• Sex life or sexual orientation<br>• Sensitive personal data does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:<br>Under the control of official authority; or<br>Authorised by domestic law<br>• The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:<br>• The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health and research. |

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

## 4. The Data Controller

4.1 The King's School processes personal data relating to parents, students, staff, trustees, visitors and others, and therefore is a data controller.

4.2 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 Board of Trustees

The Board of Trustees 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, developing related policies and guidelines where applicable and carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.

They will provide an annual report of their activities directly to the Board of Trustees 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.

Our DPO is SchoolPro TLC Limited and is contactable via DPO@SchoolPro.UK

The School's Senior Responsible Individual is the Director of Finance & Operations and is contactable via office@thekings.devon.sch.uk or 01404 812 982

### 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)
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

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.

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

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

### 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 retention schedule which can be found in Appendix 2.

## 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 student 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 students – 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 obligationsResearch and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

Data may be disclosed to the following third parties without consent:

**Other schools**
If a student transfers from The King's School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition
from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

**Local authorities**
Data may be exchanged with Local Authorities such as Devon County Council or their agents to support them with their statutory responsibilities, for example with attendance and destination information.

**Examination authorities**
This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

**Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

**Police and courts**
If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

**Social workers and support agencies**
In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

**Department for Education**
Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

**Right to be Forgotten:**
Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

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.

Formal written data processing agreements will be established before any personal data or sensitive personal data is transferred to a third party

## 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/SRI

**9.2 Children and subject access reque**

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 students at our school may not be granted without the express permission of the student. This is not a rule and a student'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 calendar 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 calendar 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 student 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 an Academy, there is no automatic right of access for those with parental responsibility to the education record of their child. The King's School will however provide free access to a student's educational record to those with parental responsibility within 15 school days upon the DPO receiving a written request.

## 11. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use fingerprints 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. 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 students 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 students. For example, students can pay for school dinners using a card system at each transaction if they wish.

Parents/carers and students 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 student 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 student'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 Director of Finance & Operations.

## 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, or students aged 13 and over, for photographs and videos to be taken of students 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 student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

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

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

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

Parents and others attending school events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the school.

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

## 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 sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at least termly
- All computer screens are locked when not in use by the person logged in
- Encryption software is used to protect all portable devices such as laptops and mobile phones
- Removable media, such as USB devices should only be used for transferring videos, lesson planning etc and not used for transferring personal data.
- Staff, students or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT policy acceptable use agreement).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

The King's 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 Old Kingsonians; and to serve as a research resource for all interested in the history of The King's 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 students eligible for pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft or loss of a school laptop or memory stick containing non-encrypted personal data about students

## 18. Training

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

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 DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every year.

## 20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Computer Security and Acceptable Use Policy
- Cyberbullying 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 DPO
- The DPO will investigate the reportand determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

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

- The 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 schools ICT 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 DPO 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

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

**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.

**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: Data / Records Retention Schedule – Based on Information and Records Management Society Guidelines

| 1.0 Board of Trustees Documentation | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| Agendas for Board of Trustees meetings | There may be data protection issues if the meeting is dealing with confidential issues relating to staff | | Permanent<br>One copy should be retained with the master set of documentation – Electronic or Paper | Secure Disposal (Shredding or Secure waste Disposal) |
| Minutes of Board of Trustees Meeting | There may be data protection issues if the meeting is dealing with confidential issues relating to staff | | Permanent for Principal Set<br>Inspection Copies – Date of meeting + 3 Years | Secure Disposal (Shredding or Secure waste Disposal) |
| Reports presented to the Board of Trustees | There 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 permanently. | Secure Disposal (Shredding or Secure waste Disposal) or retain with the signed set of the minutes. |
| Instruments of Government including Articles of Association | No | | Permanent | These should be retained in the school whilst the school is open |
| Trustees Action Plans | No | | Date of action plan + 3 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Policy documents | No | | Life of the policy + 3 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Records relating to complaints dealt with by the Board of Trustees | Yes | | Date of resolution of complaint + 6 years | Retain in school for the first six years Review for further retention in the case of contentious disputes |
| Annual Reports created under the requirements of the Education Regulations 2002 | No | Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171 | Date of report + 10 years | Secure Disposal (Shredding or Secure waste Disposal) |

| 2.0 Headteacher and Senior Leadership Team | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| 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 | Secure Disposal (Shredding or Secure waste Disposal). These could be of permanent historical value and should be offered to the County Archives Service if appropriate. |
| Minutes of Senior Leadership Team meetings | 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 (Shredding or Secure waste Disposal) |
| 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 (Shredding or Secure waste Disposal) |
| Records created by the HT, DHT, HoH or HoD. | There may be data protection issues if the report refers to individual pupils or members of staff | | Current academic year + 6 years then review | Secure Disposal (Shredding or Secure waste Disposal) |
| Correspondence created by the HT, DHT, HoH or HoD. | 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 (Shredding or Secure waste Disposal) |
| Professional Development Plans | Yes | | Life of the plan + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| School Development Plans | No | | Life of the plan + 3 years | General Disposal |

| 2.0 Admissions | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| All records relating to the creation and implementation of the School Admissions' Policy | No | School Admissions Code Statutory guidance for admission authorities | Life of the policy + 3 years then review | General Disposal |
| Admissions – if the admission is successful | Yes | School Admissions Code Statutory guidance for admission authorities | Date of admission + 1 year | Secure Disposal (Shredding or Secure waste Disposal) |
| Admissions – if the appeal is unsuccessful | Yes | School Admissions Code Statutory guidance for admission authorities | Resolution of case + 1 year | Secure Disposal (Shredding or Secure waste Disposal) |
| Register of Admissions | Yes | School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities | Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made | Secure Disposal (Shredding or Secure waste Disposal) |
| Admissions – Secondary Schools – Casual | Yes | | Current year + 1 year | Secure Disposal (Shredding or Secure waste Disposal) |
| Proofs of address supplied by parents as part of the admissions process | Yes | School Admissions Code Statutory guidance for admission authorities | Current year + 1 year | Secure Disposal (Shredding or Secure waste Disposal) |
| Supplementary Information form including additional information such as religion, medical conditions etc | Yes | | For Successful Admissions: This information should be added to the pupil file<br><br>For Unsuccessful admissions: Until Appeal process completed | Secure Disposal (Shredding or Secure waste Disposal) |

| 3.0 General Administration | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| Records relating to the creation and publication of the school prospectus | No | | Current year + 3 years | General Disposal |
| Records relating to the creation and distribution of circulars to staff, parents or pupils | No | | Current year + 1 year | General Disposal |
| Newsletters and other items with a short operational use | No | | Current year + 1 year | General Disposal |
| Visitors' Books and Signing in Sheets | Yes | | Current year + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Records relating to the creation and management of Parent Teacher Associations | No | | Current year + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |

| 4.0 Human Resources - Recruitment | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| All records leading up to the appointment of a new headteacher | Yes | | Date of appointment + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| 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 (Shredding or Secure waste Disposal) |
| All records leading up to the appointment of a new member of staff – successful candidate | Yes | | All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months | Secure Disposal (Shredding or Secure waste Disposal) |
| Pre-employment vetting information – DBS Checks | No | DBS Update Service Employer Guide Keeping children safe in education Statutory Guidance | The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months | Secure Disposal (Shredding or Secure waste Disposal) |
| Proofs of identity collected as part of the process of completing 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 placed on the member of staff's personal file | Secure Disposal (Shredding or Secure waste Disposal) |
| Pre-employment vetting information – Evidence proving the right to work in the United Kingdom | Yes | An employer's guide to right to work checks - Home Office Statutory Guidance | 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 two years | Secure Disposal (Shredding or Secure waste Disposal) |

| 4.1 Human Resources – Operational Staff Management | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| Staff Personal File | Yes | Limitation Act 1980 (Section 2) | Termination of Employment + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Timesheets | Yes | | Current year + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Annual appraisal/ assessment records | Yes | | Current year + 5 years | Secure Disposal (Shredding or Secure waste Disposal) |

| 4.2 Human Resources – Management of Disciplinary and Grievance Processes | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| Allegation of a child protection nature against a member of staff including where the allegation is unfounded | Yes | Keeping children safe in education Statutory guidance for schools and colleges | Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found,they are to be kept on the file and a copy provided to the person concerned. | Secure Disposal (Shredding or Secure waste Disposal) |
| Disciplinary Proceedings | Yes | | Trustees records will be as per the trustees' retention schedule. Formal warnings will be as per the Warning notice issued by the disciplinary panel. | Secure Disposal (Shredding or Secure waste Disposal) |

| 5.0 Health and Safety | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| Health and Safety Policy Statements | No | | Life of policy + 3 years | General Disposal |
| Health and Safety Risk Assessments | No | | Life of risk assessment + 3 years unless accident or injury occurs | General Disposal |
| Records relating to accident/ injury at school or on trip | Yes | | Date of incident + 12 years<br>In the case of serious accidents, a further retention period will need to be applied | Secure Disposal (Shredding or Secure waste Disposal) |
| Accident reporting | Yes | Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration<br>Act 1992 Section 8. Limitation Act 1980 | Adults: Date of the incident + 6 years<br>Children: DOB of the child + 25 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Control of Substances Hazardous to Health (COSHH) | No | Control of Substances Hazardous to Health<br>Regulations 2002. SI 2002 No 2677 Regulation 11 | Current year + 40 years | General Disposal |
| Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos | No | Control of Asbestos at Work Regulations 2012 SI<br>1012 No 632 Regulation 19 | Last action + 40 years | General Disposal |
| Fire Precautions log books | No | | Current year + 6 years | General Disposal |
| Records created by schools to obtain approval to run an Educational Visit outside the Classroom | No | Outdoor Education Advisers' Panel National<br>Guidance website - Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice". | Date of visit + 10 years | Secure Disposal (Shredding or Secure waste Disposal) |

| | | | | |
|---|---|---|---|---|
| Parental consent forms for school trips where there has been no major incident | Yes | | Conclusion of the trip | Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low. |
| Parental permission slips for school trips – where there has been an incident | Yes | Limitation Act 1980 (Section 2) | DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils | Secure Disposal (Shredding or Secure waste Disposal) |

| 6.0 Financial and Asset Management | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| Employer's Liability Insurance Certificate | No | | Closure of the school + 40 years | General Disposal |
| Asset Inventory | No | | Current year + 6 years | General Disposal |
| Reports of Burglary, theft and vandalism | No | | Current year + 6 years | General Disposal |
| All records relating to the management of contracts under signature / seal | No | Limitation Act 1980 | Under Seal: Last payment on the contract + 12 years<br>Under Signature: Last payment on the contract + 6 years | General Disposal |
| Annual Accounts | No | | Current year + 6 years | General Disposal |
| Loans and grants managed by the school | No | | Date of last payment on the loan + 12 years | General Disposal |
| Student financial support applications | Yes | | Current year + 3 years | Secure Disposal (Shredding or Secure waste Disposal) |
| All records relating to the creation and management of budgets including the Annual Budget statement and background papers | Yes – Staffing Data | | Life of the budget + 3 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Invoices, receipts, order books and requisitions, delivery notices | No | HMRC | Current financial year + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Records relating to the collection and banking of monies and processing of card payments | No | HMRC | Current financial year + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Payroll information, with statutory payment details | Yes | HMRC & Statutory Maternity Pay (General) Regulations 1986 | Current financial year + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |

| 7.0 Property Management | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| Title deeds of properties belonging to the school | No | | Permanent | |
| Plans of property belong 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. | |
| Leases of property leased by or to the school | No | | Expiry of lease + 6 years | General Disposal |
| Records relating to the letting of school premises | No | | Current financial year + 6 years | General Disposal |
| All records relating to the maintenance of the school carried out by contractors | No | | Current year + 6 years | General Disposal |
| All records relating to the maintenance of the school carried out by school employees | No | | Current year + 6 years | General Disposal |

| 8.0 Pupil Management | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| 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<br><br>Limitation Act 1980 (Section 2) | Date of Birth of the pupil + 25 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Examination Results – Pupil Copies | Yes | | This information should be added to the pupil file | All uncollected certificates should be returned to the examination board |
| Child Protection information held on pupil file | Yes | Keeping children safe in education Statutory guidance for schools and colleges | 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 |
| Child protection information held in separate files | Yes | Keeping children safe in education Statutory guidance for schools and colleges | DOB of the child + 25 years then review<br>This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record | SECURE DISPOSAL – these records MUST be shredded |
| Attendance Registers | Yes | School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities | Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made. | Secure Disposal (Shredding or Secure waste Disposal) |
| Correspondence relating to authorized absence | Yes | Education Act 1996 Section 7 | Current academic year + 2 years | Secure Disposal (Shredding or Secure waste Disposal) |

| | | | | |
|---|---|---|---|---|
| Special Educational Needs files, reviews and Individual Education Plans | Yes | Limitation Act 1980 (Section 2) | Date of Birth of the pupil + 25 years | REVIEW<br>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 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 and this should be documented. |
| 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 (Shredding or Secure waste Disposal) |
| 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 (Shredding or Secure waste Disposal) |
| 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 (Shredding or Secure waste Disposal) |

| 9.0 Curriculum | | | | |
|---|---|---|---|---|
| **Basic file description** | **Data Protection Issues** | **Statutory Provisions** | **Retention Period** | **Action at the end of the retention period** |
| Examination Results (Schools Copy) | Yes | | Current year + 3 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Examination Papers | Yes | | The examination papers should be kept until any appeals/validation process is complete | Secure Disposal (Shredding or Secure waste Disposal) |
| Published Admission Number (PAN) Reports | Yes | | Current year + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Value Added and Contextual Data | Yes | | Current year + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Self-Evaluation Forms | Possibly | | Current year + 6 years | Secure Disposal (Shredding or Secure waste Disposal) |
| Schemes of Work | No | | Current year + 1 year | General Disposal |
| Timetable | No | | Current year + 1 year | General Disposal |
| Mark Books | No | | Current year + 1 year | General Disposal |
| Record of homework set | No | | Current year + 1 year | General Disposal |
| Pupils' Work | No | | Where possible pupils' work should be returned to the pupil at the end of the academic year or current year + 1 year | General Disposal |