University of Birmingham School

Data Protection Policy

March 2024

University of Birmingham School Data Protection Policy

Review Frequency	Annually	**Review date**	March 2024
Governing Committee Responsible	Resources Committee	**Next Due**	March 2025
Governor Approval (date)	13 March 2024	**Website**	Yes
Employees Responsible	C Townsend	**Date Produced**	

At University of Birmingham School we refer to **Pupils** (who are in Years 7-11 and aged 11-16) and **Students** (who are in Years 12/ 13 and aged 17-18)

1. Aims

Our School aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- https://www.gov.uk/data-protection (the Data Protection Act 2018).

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

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 regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

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, living individual. This may include the individual's: › Name (including initials) › Identification number › Location data › Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

TERM	DEFINITION
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 personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

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

The School has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

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

5.1 Governing board

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

5.2 Data protection officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on School data protection issues.

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

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

Our DPO is Judicium and is contactable via dataservices@judicium.com

5.3 School Business Leader

The School Business Leader 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 UK
    - 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 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

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

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

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

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

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

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

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

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.

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the School's record retention schedule.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

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

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

Where we transfer personal data internationally, we will do so in accordance with UK 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

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

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

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

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 (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it

- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

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

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

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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. Parental requests to see the educational record

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

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

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

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

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints 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 1 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. For example, pupils can pay for School dinners via debit card / contactless at each transaction if they wish.

Parents/carers and pupils can 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 follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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

Any enquiries about the CCTV system should be directed to a member of the Senior Leadership Team in the first instance.

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

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

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

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

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

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

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chat-bots such as ChatGPT and Google Bard. University of Birmingham School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chat-bots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, University of Birmingham School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our School and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept 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, 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 10 characters long containing letters and numbers are used to access School computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- 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 of ICT Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will 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.

18. 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 after becoming aware of it. Such breaches in a School context may include, but are not limited to:

- A non-anonymised dataset being published on the School website, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a School laptop containing non-encrypted personal data about pupils

19. 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.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

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

21. Links with other policies

This data protection policy is linked to the School's:

- Freedom of information Policy
- CCTV Policy
- Acceptable Use of ICT Policy
- Safeguarding Policy
- Media Consent Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by emailing them at dataservice@judicium.com
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal / School Business Leader and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Shared Drive.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the School's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the School's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- Where the School is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to 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 on the Shared Drive
- The DPO and Principal / School Business Leader will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and Principal / School Business Leader will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the School to reduce risks of future breaches

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the 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 Network Manager to attempt to recall it from external recipients and remove it from the School's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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 endeavor to obtain 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

- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the School should inform any, or all, of its 3 local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the School website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A School laptop containing non-encrypted sensitive personal data being stolen or hacked
- The School's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Appendix2 – Data Retention Guidance

The below table provides guidance for how long records should be retained.

Basic file description	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Child Protection			
Child Protection files	Education Act 2012, s175, related guidance "Keeping Children Safe in Education"	DOB + 25 years	SECURE DISPOSAL
Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL
Governors			
Minutes - Principal set (signed)		Permanent	Retain in School for 6 years from date of meeting
Minutes - Inspection copies		Date of meeting + 3 years	SECURE DISPOSAL [If these minutes contain any sensitive personal information they should be shredded]
Agendas		Date of meeting	SECURE DISPOSAL
Reports		Date of report + 6 years	Retain in School for 6 years from date of meeting

Instruments of Government		Permanent	Retain in School whilst School is open
Trusts and Endowments		Permanent	Retain in School whilst operationally required
Action Plans		Date of action plan + 3 years	SECURE DISPOSAL
Policy documents		Expiry of policy	Retain in School whilst policy is operational (this includes if the expired policy is part of a past decision making process)
Complaints files		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 SECURE DISPOSAL routine complaints
Annual Reports required by the Department for Education	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	
Management			
Log Books		Date of last entry in the book + 6 years	Retain in the School for 6 years from the date of the last entry
Minutes of the Senior Management Team and other internal administrative bodies		Date of meeting + 5 years	Retain in the School for 5 years from meeting
Reports made by the Principal or the Senior Leadership Team		Date of report + 3 years	Retain in the School for 3 years from meeting
Records Principal, Senior and Middle Leaders another members of staff with administrative responsibilities		Closure of file + 6 years	SECURE DISPOSAL

Correspondence created by Principal, Senior and Middle Leaders and other members of staff with administrative responsibilities		Date of correspondence + 3 years	SECURE DISPOSAL
Professional Development Plans		Closure + 6 years	SECURE DISPOSAL
School Development Plans		Closure + 6 years	Review
Admissions - if the admission is Successful	Yes	Admission + 1 year	SECURE DISPOSAL
Admissions - if the appeal is Unsuccessful	Yes	Resolution of case + 1 year	SECURE DISPOSAL
Admissions - Secondary Schools - Casual		Current year + 1 year	SECURE DISPOSAL
Proofs of address supplied by parents as part of the admissions process		Current year + 1 year	SECURE DISPOSAL
Pupils			
Admission Registers		Date of last entry in the book (or file) + 6 years Re considers Retention Period. Feedback from Teaching Relative was thought to be 7 Year Retention. These records are no longer generated in paper but electronically held using SIMS software.	Retain in the School for 6 years from the date of the last entry then consider transfer to the Archives
Attendance registers		Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any backup copies

			should be destroyed at the same time]
Pupil Files Retained in Schools	Limitation Act 1980	DOB of the pupil + 25 years	SECURE DISPOSAL
Pupil Files	Limitation Act 1980	DOB of the pupil + 25 years	SECURE DISPOSAL
Special Educational Needs Files, reviews and Individual Education Plans		DOB of the pupil + 25 years the review NOTE: This retention period is the minimum 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.	SECURE DISPOSAL
Correspondence Relating to Authorized Absence and Issues		Date of absence + 2 years	SECURE DISPOSAL
Examination results – Public		Year of examinations + 6 years	SECURE DISPOSAL
Examination results – Internal		Current year + 5 years	SECURE DISPOSAL
Any other records created in the course of contact with pupils		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL
Statement maintained under The Education Act 1996 - Section 324	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
Proposed statement or amended statement	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending

Advice and information to parents regarding educational needs	Special Educational Needs and Disability Act 2001 Section 1	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
Accessibility Strategy	Special Educational Needs and Disability Act 2001 Section 1	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
Parental permission slips for School trips - where there has been no major incident		Conclusion of the trip	SECURE DISPOSAL
Parental permission slips for School trips - where there has been a major incident.	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL
Records created by Schools to obtain approval to run an Educational Visit outside the Classroom	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years	SECURE DISPOSAL
Walking Bus registers		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any backup copies should be destroyed at the same time]
Curriculum			
School Development Plan		Current year + 6 years	SECURE DISPOSAL
Curriculum returns		Current year + 3 years	SECURE DISPOSAL
Schemes of work		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL

Timetable		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Class record books		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Mark Books		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Record of homework set		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Pupils' work		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Examination results		Current year + 6 years	SECURE DISPOSAL
SATS records - Examination Papers and Results		Current year + 6 years	SECURE DISPOSAL
PAN reports		Current year + 6 years	SECURE DISPOSAL
Value Added & Contextual Data		Current year + 6 years	SECURE DISPOSAL
Self-Evaluation forms		Current year + 6 years	SECURE DISPOSAL
Personnel Records held in Schools			
Timesheets, sick pay	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Staff Personal files		Termination + 7 years	SECURE DISPOSAL
Interview notes and recruitment records		Date of interview + 6 months	SECURE DISPOSAL
Pre-employment vetting information (including DBS	DBS guidelines	Date of check + 6 months	SECURE DISPOSAL

checks)			
Disciplinary proceedings: oral warning	Where the warning relates to child protection issues see Child Protection. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.	Date of warning + 6 months	SECURE DISPOSAL
Disciplinary proceedings: written warning	Where the warning relates to child protection issues see Child Protection. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.	Date of warning + 6 months	SECURE DISPOSAL
Disciplinary proceedings: final written warning	Where the warning relates to child protection issues see Child Protection. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.	Date of warning + 12 months	SECURE DISPOSAL
Disciplinary proceedings: case not found	Where the warning relates to child protection issues see Child Protection. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.	If child protection related please see child protection, otherwise SECURE DISPOSAL immediately at the conclusion of the case	SECURE DISPOSAL
Records relating to accident/ injury at work		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL

Annual Appraisal and Assessment Records		Current year + 5 years	SECURE DISPOSAL
Salary cards		Last date of employment + 85 years	SECURE DISPOSAL
Maternity pay records	Statutory Maternity Pay (General) Current year +3yrs Regulations 1986 (SI 1986/ 1960), revised 1999 (SI 1999/ 567)	Current year +3yrs	SECURE DISPOSAL
Records held under Retirement benefits Schemes (Information Powers) Regulations 1995		Current year + 6 years	SECURE DISPOSAL
Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure		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
Health and Safety			
Accessibility Plans		Current year + 6 years	SECURE DISPOSAL
Accident Reporting – Adults		Date of incident + 7 years	SECURE DISPOSAL
Accident Reporting - Children		DOB of child + 25 years	SECURE DISPOSAL
COSHH		Current year + 10 years [where appropriate an additional retention period may be allocated]	SECURE DISPOSAL
Incident reports		Current year + 20 years	SECURE DISPOSAL
Policy Statements		Date of expiry + 1 year	SECURE DISPOSAL
Risk Assessments		Current year + 3 years	SECURE DISPOSAL
Process of monitoring of areas where employees and persons are		Last action + 40 years	SECURE DISPOSAL

likely to have become in contact with asbestos			
Process of monitoring of areas where employees and persons are likely to have come in contact with radiation		Last action + 50 years	SECURE DISPOSAL
Fire Precautions log books		Current year + 6 years	SECURE DISPOSAL
Administrative			
Employer's Liability certificate		Closure of the School + 40 years	SECURE DISPOSAL
Inventories of equipment & furniture		Current year + 6 years	SECURE DISPOSAL
General file series		Current year + 5 years	Review to see whether a further retention period is required
School brochure or prospectus		Current year + 3 years	Review to see whether a further retention period is required
Circulars (staff/ parents/ pupils)		Current year + 1 year	SECURE DISPOSAL
Newsletters, ephemera		Current year + 1 year	Review to see whether a further retention period is required
Visitors book		Current year + 2 years	Review to see whether a further retention period is required
PTA/ Old Pupils Associations		Current year + 6 years	Review to see whether a further retention period is required
Finance			
Annual Accounts	Financial Regulations	Current year + 6 years	
Loans and grants	Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required
Contracts - under seal		Contract completion date + 12 years	SECURE DISPOSAL
Contracts - under signature		Contract completion date + 6 years	SECURE DISPOSAL
Contracts - monitoring records		Current year + 2 years	SECURE DISPOSAL
Copy orders		Current year + 2 years	SECURE DISPOSAL

Budget reports, budget monitoring etc.		Current year + 3 years	SECURE DISPOSAL
Invoice, receipts and other records covered by the Financial Regulations	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Annual Budget and background papers		Current year + 6 years	SECURE DISPOSAL
Order books and requisitions		Current year + 6 years	SECURE DISPOSAL
Delivery Documentation		Current year + 6 years	SECURE DISPOSAL
Debtors' Records	Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL
School Fund - Cheque books		Current year + 3 years	SECURE DISPOSAL
School Fund- Paying in books		Current year + 6 years then review	SECURE DISPOSAL
School Fund - Ledger		Current year + 6 years then review	SECURE DISPOSAL
School Fund - Invoices		Current year + 6 years then review	SECURE DISPOSAL
School Fund - Receipts		Current year + 6 years	SECURE DISPOSAL
School Fund - Bank statements		Current year + 6 years then review	SECURE DISPOSAL
School Fund- School Journey books		Current year + 6 years then review	SECURE DISPOSAL
Student grant applications		Current year + 3 years	SECURE DISPOSAL
Free School meals registers		Current year + 6 years	SECURE DISPOSAL
Petty cash books		Current year + 6 years	SECURE DISPOSAL
Property			
Title Deeds		Permanent	Permanent, these should follow the property unless the property has been registered at the Land Registry
Plans		Permanent	Retain in School whilst operational
Maintenance and contractors	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Leases		Expiry of lease + 6 years	SECURE DISPOSAL
Lettings		Current year + 3 years	SECURE DISPOSAL

Burglary, theft and vandalism report forms		Current year + 6 years	SECURE DISPOSAL
Maintenance log books		Current year + 6 years	SECURE DISPOSAL
Contractors' Reports		Current year + 6 years	SECURE DISPOSAL
Department for Education			
OFSTED reports and papers		Replace former report with any new inspection report	Review to see whether a further retention period is required
Returns		Current year + 6 years	SECURE DISPOSAL
Schools Meals			
Dinner Register		Current year + 3 years	SECURE DISPOSAL
School Meals Summary Sheets		Current year + 3 years	SECURE DISPOSAL

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 report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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 before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (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
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the School's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the School's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the School is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to 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 Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and Principal will meet to assess recorded data breaches and identify any trends or patterns requiring action by the School to reduce risks of future breaches

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the 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/ external IT support provider] to attempt to recall it from external recipients and remove it from the School's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorized 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 endeavour to obtain 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