DATA PROTECTION POLICY

DATE APPROVED	BODY	REVIEW DATE
15th September 2020	Board of Trustees	Autumn 2022
16th September 2022	Board of Trustees	Autumn 2023
14th September 2023	Board of Trustees	Autumn 2024
12th December 2024	Board of Trustees	Autumn 2025
11th December 2025	Board of Trustees	Autumn 2 2026

Contents

1. Aims 3
2. Legislation And Guidance 3
3. Definitions 3
4. The Data Controller 4
5. Roles and Responsibilities 4
    5.1 The Trust's Board of Trustees 4
    5.2 Data protection officer (DPO) 4
    5.3 Data protection lead (DPL) 4
    5.4 Local Governing Body 4
    5.6 All staff 5
6. Data Protection Principles 5
7. Collecting Personal Data 5
    7.1 Lawfulness, fairness and transparency 5
    7.2 Limitation, minimisation and accuracy 6
8. Sharing Personal Data 6
9. Subject Access Requests and Other Rights Of Individuals 7
    9.1 Subject access requests 7
    9.2 Children and subject access requests 7
    9.3 Responding to subject access requests 8
    9.4 Other data protection rights of the individual 8
10. Parental Requests To See The Educational Record 8
12. CCTV 9
13. Photographs and videos 9
14. Artificial Intelligence (AI) 9
15. Data Protection By Design And Default 10
16. Data Security And Storage Of Records 10
17. Disposal of records 11
18. Personal data breaches 11
19. Training 11
20. Monitoring Arrangements 11
21. Links With Other Policie 11
Appendix 1: Data Management and Retention Policy 12
Appendix 2 : Personal Data Breach Procedure 14
    Actions to minimise the impact of data breaches 15
Appendix 3: School Specific Information and Check List 16

1. Aims

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

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 GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 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 also reflects the ICO's guidance for the use of surveillance cameras and personal information.

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

3. Definitions

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

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

4. The Data Controller

Our schools and organisations process personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore the trust is classed as the data controller with the schools and organisations as trading names.

The trust 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 schools, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Trust's Board of Trustees

The Trust board has overall responsibility for ensuring that our schools/organisations comply 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 trust board and, where relevant, report to the board their advice and recommendations on trust and school/organisation data protection issues.

The data protection officer is employed by the Chiltern Learning Trust. (please see appendix 3 for details)

5.3 Data protection lead (DPL)

A named data protection lead (DPL) will be appointed at each school or organisation within the trust and they will be responsible for the day to day monitoring of their procedures to ensure compliance with the data protection law. Guidance will be provided by the data protection officer (DPO) in order to support the DPL within each establishment.

The DPL is the first point of contact for individuals whose data the school/organisation processes, and should raise concerns and breaches with the trust DPO. The DPO will make any required contact with the ICO.

See Appendix 3 for the name of our DPL and details of how to contact them.

5.4 Local Governing Body

The local governing body of each school or organisation is responsible for ensuring compliance with the data protection policy within its establishment.

5.5 Headteacher

The local governing body delegates the day to day responsibility to the Headteacher to act as the representative of the data controller in accordance with the Trust's Scheme of Delegation.

5.6 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school/organisation of any changes to their personal data, such as a change of address
- Contacting the DPL in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the 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 Trust and its schools/organisations must comply with the UK GDPR data protection principles:

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 Trust through its schools/organisations 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 six '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 one 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 effect 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 Policy.

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 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 Trust 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 must 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 DPL.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

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

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within1 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 unless the request is unfounded or excessive, in which case 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. This does not apply to requests made under the Education Regulations 2005.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information 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, at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's 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

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 and there is no other legal ground for processing the data.
- Ask us to rectify, erase or restrict processing of their personal data, (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- 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 DPL. If staff receive such a request, they must immediately forward it to the DPL.

10. Parental Requests To See The Educational Record

Parents or those with parental responsibility do not have an automatic parental right of access to their child's education record from an academy, free or independent school but the Chiltern Learning Trust will provide these details (which includes most information about a pupil) within 15 school days of receipt of a written

request under the Education Regulations 2005, which does not affect personal data under data protection legislation or GDPR or the Trust Privacy Notices.

The Trust may charge a fee to cover the cost of supplying the educational record in these circumstances.

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

There are certain circumstances in which this request 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.

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. Full details on CLT's CCTV Policy are available on the trust website.

Please refer to Appendix 3 for details of the designated contact for all CCTV system enquiries

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 for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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

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 chatbots such as ChatGPT and Google Gemini. The Chiltern Learning Trust recognises that AI has many uses to help pupils learn and support staff workload, 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 any generative AI tools or chatbots apart from Gemini and Notebook LM (provided as part of Google Workspace for Education when using your trust supplied google login), in line with our AI Policy. Using non approved AI tools risks data breaches as many of the free tools retain and train the AI models on inputted data.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, The Chiltern Learning Trust 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 at trust level and DPL within each school/organisation, 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) via the DPL.
- 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 will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school/organisation and DPL 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 staff room 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 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 **[online safety policy/ICT policy/acceptable use agreement/policy on acceptable use/ESafety and Acceptable Use Policy])**
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

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 trust and its schools/organisations 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 board of trustees.The annual review frequency reflects the Department of Education's recommendations in its advice on statutory policies.

21. Links With Other Policies

This data protection policy is linked to our:

- Freedom of Information Policy
- Code of Conduct for Employees
- Internet and Email Acceptable Use Policy
- Safeguarding (including child protection) Policy
- CCTV Policy
- Privacy notices

See appendix 3 for details of any other school relevant policies

Appendix 1: Data Management and Retention Policy

1. About this policy

The Chiltern Learning Trust ("the Trust) recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of our schools. Good record keeping should protect the rights of all and provide evidence for demonstrating performance and accountability. This policy provides the framework to achieve effective management and audit of records.

2. Scope

This policy applies to all records created, received or maintained by permanent and temporary staff of the Trust in the course of carrying out its functions; and also, by any agents, contractors, consultants or third parties acting on its behalf.

Records are defined as all those documents which facilitate the business carried out by the school trust and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronic format e.g. paper documents, scanned documents, e-mails, audio and video recordings, text messages, notes of telephone and spreadsheets, documents, presentations etc.

3. Legislation and Guidance

This policy meets the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000 (FOIA 2000). It is based on the IRMS Toolkit for Schools for retention guidelines. By following this, the Trust will ensure they are compliant with management and retention of data within the legislative requirements in the aforementioned Acts.

4. Responsibilities

4.1 The Trust

The governing body of the Trust has a statutory responsibility to maintain the records and record keeping systems in accordance with the regulatory environment specific to the Trust.

4.2 The Local Governing Board

The Trust has delegated this responsibility to the local governing body in each of its schools/organisations, which has delegated day to day responsibility for this to the Headteacher of the establishment, in accordance with the Trust's Scheme of Delegation.

4.3 The Data Protection Lead

The Data Protection Lead/operational management in the Trust/school will give guidance on good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way.

They will also monitor compliance with this policy by auditing at least annually the creation, holding, receiving and use of data to check if records are stored securely and can be accessed appropriately. This will ensure records are managed to get the most effective business use from them.

Records will be managed in line with the Records Retention Schedule. This will help ensure the Trust can meet its responsibilities under the data protection and FoI legislation.

4.4 All Staff

Individual staff and employees must ensure, with respect to records for which they are responsible, that they:

- Manage the Trust's records consistently in accordance with the Trust's policies
- Hold all records with appropriate security in line with all Trust policies.
- Only share any records appropriately and not disclose any records to any unauthorised third party
- Dispose of all records in accordance with the Trust's Records Retention Schedule

5. Digital communications management

As communicating by email or on digital platforms is quick and easy, the language used can often be less formal and more open to misinterpretation. Follow these guidelines:

- Use spell check and consider how the recipient will view the wording you have used
- Turn off the autocomplete feature in the "To" box as this is the most common data breach sending emails to the wrong recipients
- Ensure that Bcc is used where appropriate to avoid the unauthorised disclosure of email addresses of intended recipients
- When sending confidential or sensitive information it should be sent using a secure encrypted system. If this is not possible please contact your DPL. Only include information that is needed
- All digital records including digital communications must be stored in line with the Trust's RRS.

All digital communications are subject to SARs and FoI requests and are to be disclosed if requested.

6. Safe Destruction of Records

All records at the end of their retention period must be reviewed and destroyed in accordance with this policy.

The disposal or paper records should be via a cross-cutting shredder onsite. If an external provider is used, all paper records will also be shredded on site.

Physical media used to store electronic records that require secure disposal will be shredded to a maximum particle size of 6mm to ensure no data is able to be recovered from the devices.

7. Relationship with Existing Policies

This policy has been drawn up within the context of:

- Data Protection Policy
- Records Retention Schedule
- ICT and Internet Acceptable Use Policy
- Social Media Policy
- Cyber Security Protocol
- Keeping Children Safe in Education

Appendix 2 : 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 Data Protection Lead within the school/organisation who will then contact the trust Data Protection Officer (DPO).
- The trust 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 trust DPO will alert the CEO and the Board of Trustees
- 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 DPL and DPO with this where necessary and the DPO should take external advice when required.
- 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. 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 using the ICO's self-assessment tool., 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 by the trust on Google Drive.
- Where the ICO must be notified, the DPO will do this via the report a breach page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours 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/organisation'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/organisation 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 relating to the breach
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored in a secure location by the DPO.
- The DPO, DPL and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- The DPL and Headteacher 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 DPL as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the [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 or cannot be confirmed as successful, the DPL will inform the DPO who 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 DPL will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPL will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPL will inform the designated safeguarding lead as well as the DPO and discuss whether the school should inform any, or all, of its local safeguarding partners

Appendix 3: School Specific Information and Checklist

Please complete the table below with your school specific information

5.2 The data protection officer is	Chris Beeden
5.3 Our DPL is	Sharon Keely
5.3 Our DPL is contactable via	office@springfieldprimaryschool.org.uk
12. Enquiries about CCTV system directed to	Sharon Keely
21. Any other school relevant policies	● Data Protection Policy ● Records Retention Schedule ● ICT and Internet Acceptable Use Policy ● Social Media Policy ● Cyber Security Protocol ● Keeping Children Safe in Education