CHOSEN HILL SCHOOL

DATA PROTECTION POLICY

Committee Assigned:	**Community and People**
Type of Policy:	**STATUTORY**
Date approved:	**June 2018**
Date reviewed:	**April 2020**
Date for review:	**June 2022**
SLT Author:	**DWR**

Contents

1. Aims

Chosen Hill School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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 GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

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

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

In addition, this policy complies with the school's funding agreement and Articles of Association.

3. Definitions

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

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

4. The data controller

Chosen Hill school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Governing Body

The governing Body has overall responsibility for ensuring that the school complies with all relevant data protection obligations. A Governor has been appointed for specific GDPR responsibilities and reports to the Resources Committee. There is a standing agenda item for GDPR.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the school's 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 Body and, where relevant, report to the Governors 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.

The school's DPO is SchoolPro TLC limited and they are contactable via GDPR@schoolpro.co.uk

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
    - If there has been a data breach;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The GDPR is based on data protection principles that Chosen Hill 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

Chosen Hill School will only process personal data where the school has one of 6 'lawful bases' (legal reasons) to do so under data protection law:

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

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

If the school offers online services to pupils, such as classroom apps, and the school intends to rely on Public Task as a basis for processing, where this is not appropriate the school will get parental consent for processing (except for online counselling and preventive services).

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

7.2 Limitation, minimisation and accuracy

The school will only collect personal data for specified, explicit and legitimate reasons. The school will explain these reasons to the individuals when the school first collects their data.

If the school wants to use personal data for reasons other than those given when the school first obtained it, the school will inform the individuals concerned before the school does so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's records management policy.

7.3 The school's processing of special categories of personal data and criminal offence data

As part of the school's statutory functions, the school processes special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special Category Data
Special category data is defined at Article 9 GDPR as personal data revealing:

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

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

Appropriate Policy Document
Some of the Schedule 1 conditions for processing special category and criminal offence data require the school to have an Appropriate Policy Document ('APD') in place, setting out and explaining the school's procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.
This section of the school's Data Protection Policy document explains the school's processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.
In addition, it provides some further information about the school's processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements the school's privacy notice and staff privacy notice.

Conditions for processing special category and criminal offence data
The school processes special categories of personal data under the following GDPR Articles:
i. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the school or the data subject in connection with employment, social security or social protection.
Examples of the school's processing include staff sickness absences.
ii. Article 9(2)(g) - reasons of substantial public interest.

The school is a publicly funded body and provides a safeguarding role to young and vulnerable people. The school's processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of the school's role.
Examples of the school's processing include the information the school seeks or receives as part of investigating an allegation.
iii. Article 9(2)(j) – for archiving purposes in the public interest.
The relevant purpose the school relies on is Schedule 1 Part 1 paragraph 4 – archiving.
An example of the schools processing is the transfers the school makes to the County Archives as set out in the school's Records Management Policy.
iv. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.
Examples of the school's processing include processing relating to any employment tribunal or other litigation.
v. Article 9(2)(a) – explicit consent
In circumstances where the school seeks consent, the school will make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.
Examples of the school's processing include staff dietary requirements and health information the school receives from the school's customers who require a reasonable adjustment to access the school's services.
vi. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.
An example of the school's processing would be using health information about a member of staff in a medical emergency.

The school processes criminal offence data under Article 10 of the GDPR
Examples of the school's processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Processing which requires an Appropriate Policy Document
Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).
This section of the policy is the APD for the school. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the GDPR Article 5 principles. The school's retention with respect to this data is documented in the school's retention schedules.

Description of data processed
The school processes the special category data about the school's employees that is necessary to fulfil the school's obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any union. Further information about this processing can be found in the school's staff privacy notice.
The school processes the special category data about the children in the school's care and other members of the school's community that is necessary to fulfil the school's obligations as a school, and for safeguarding and care. This includes information about their health and wellbeing, ethnicity, photographs and other categories of data relevant to the provision of care. Further information about this processing can be found in the school's pupil privacy notice.

The school also maintains a record of the school's processing activities in accordance with Article 30 of the GDPR.

Schedule 1 conditions for processing
Special category data
The school processes SC data for the following purposes in Part 1 of Schedule 1:

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

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

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

Criminal offence data
The school processes criminal offence data for the following purposes in parts 1, 2 and 3 of Schedule 1:

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

8. Sharing personal data

The school will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of the school's staff at risk
- The school needs to liaise with other agencies – the school will seek consent as necessary before doing this
- The school's suppliers or contractors need data to enable us to provide services to the school's staff and pupils – for example, IT companies. When doing this, the school will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data the school shares
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

- Where the disclosure is required to satisfy the school's safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

The school may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of the school's pupils or staff.

Where the school transfers personal data to a country or territory outside the European Economic Area, the school will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

A form is available from the School Business Manager or on the school website.

If staff receive a subject access request 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 Chosen Hill 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, the school:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request

- Will provide the information free of charge
- May tell the individual the school will comply within 3 months of receipt of the request, where a request is complex or numerous. The school will inform the individual of this within 1 month, and explain why the extension is necessary

The school will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature, the school may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

When the school refuses a request, the school will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when the school is collecting their data about how the school uses and processes it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. Parental requests to see the educational record

Parents, or those with parental responsibility, do not have automatic parental right of access to their child's educational record but the school may choose to provide this. Please put your requests in writing to the school Data Protection Officer and requests will be evaluated on a case by case basis.

11. Biometric recognition systems

Where the school uses 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, and 6th form registration), the school will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before the school 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). The school will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using an id style card.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the school 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, the school 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), the school 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

The school uses CCTV in various locations around the school site to ensure it remains safe. The school will adhere to the ICO's code of practice for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to the Business Manager.

13. Photographs and videos

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

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

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.

- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the school's website or social media pages

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

When using photographs and videos in this way the school will not accompany them with any other personal information about the child, to ensure they cannot be identified, unless you have given us permission to do so.

See the school's child protection and safeguarding and e-safety policies for more information on the school's use of photographs and videos.

14. Data protection by design and default

The school will put measures in place to show that the school has integrated data protection into all of the school's data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; the school will also keep a record of attendance
- Regularly conducting reviews and audits to test the school's privacy measures and make sure the school is compliant
- Maintaining records of the school's processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the school's and DPO and all information the school is required to share about how the school uses and processes their personal data (via the school's privacy notices)
    - For all personal data that the school holds, maintaining an internal record of the type of data, data subject, how and why the school is using the data, any third-party recipients, how and why the school is storing the data, retention periods and how the school is keeping the data secure

15. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see the school's IT policy/acceptable use agreement)
- Where the school needs to share personal data with a third party, the school carries out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

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

For example, the school will shred or incinerate paper-based records, and overwrite or delete electronic files. The School may also use a third party to safely dispose of records on the school's behalf. If the school does so, the school will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the school will follow the procedure set out in appendix 1.

When appropriate, the school will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

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

18. Training

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

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

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect the school's practice. Otherwise, this policy will be reviewed **every 2 years** and shared with the full governing board.

20. Links with other policies

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

- Freedom of information publication scheme
- Data Retention/records management policy
- IT policy/acceptable use
- Confidentiality policy
- CCTV Policy
- Social Media protocol
- E-Safety Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

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

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

        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored within the school's GDPRiS software.

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

Actions to minimise the impact of data breaches

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

Actions will include for example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the 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 team to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure the school receives 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, the school will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2: Personal data breach Initial Report Form

School Security Breach Initial Report

Please complete this form as fully as possible within 1 working day of the breach taking place

1. Initial report

1.1 Reporter

Name:		**Job Title:**	
Head teacher:		**School:**	
Email Address:		**Phone Number:**	

1.2 Summary of the incident

Date of incident:		**Location of incident:**	

1.3 Type of information

Type of information: **e.g. Information has been sent to the wrong address**		**Number of people affected (approx if not known):**	
Is the information personal or sensitive personal information?		Choose an item.	

- "personal data" means data which relate to a living individual who can be identified—
  (a) from those data, or
  (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual; e.g. name, address, date of birth, national insurance number, NHS number, personal email address
- "Sensitive personal data" means personal data consisting of information as to—
  (a)the racial or ethnic origin of the data subject,
  (b)their political opinions,
  (c)their religious beliefs or other beliefs of a similar nature,
  (d)whether they are a member of a trade union within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992
  (e)their physical or mental health or condition,
  (f)their sexual life,
  (g)the commission or alleged commission by them of any offence, or
  (h)any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

1.4 Incident details

Briefly state what happened and who was involved in the breach? (This box will expand as you type)

1.5 Initial actions taken

What have you done to mitigate any immediate risks arising from the breach, who has been informed, have you considered whether it is appropriate to inform any individuals who may be affected and offered them the chance to make a formal complaint? (This box will expand as you type)

For example:

- Do you have confirmation that an email that was sent to the wrong recipient has been permanently deleted?
- Have you ensured the return of any files or letters that were sent to the wrong address?
- Do you have confirmation that a letter or data received by the wrong person or organisation has been destroyed?
- Have you reported a missing or stolen device (e.g. mobile phone, laptop, memory stick) to your ICT team and, if necessary, the police?
- Who have you informed? E.g. Head teacher, Business Manager, Police.

A more detailed report of the circumstances surrounding this breach and the actions undertaken to prevent further occurrences of this nature may be required following the school's initial assessment.