# Data Protection Policy
# This policy is applicable to The Schelwood Trust

Reviewed September 2026 following DfE guidance update of 9 July 2026

## Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

## Consultation/Formulation of Policy

This policy has been drawn up following the provisions of the DPA 2018.

## Related Statutory Requirements/non-statutory guidance which inform policy

General Data Protection Regulation (GDPR)
Data Protection Act 2018 (DPA 2018)
Protection of Freedoms Act 2012
ICO Code of Practice
Information Management Toolkit for Schools
Department for Education: Data protection in schools (updated 9 July 2026)
Data (Use and Access) Act 2025
Department for Education: Protection of biometric data of children in schools and colleges (June 2026)

## Link to other school/MAT policies, documents and required practice

- Freedom of information publication scheme
- ICT Acceptable Usage Policy
- Child Protection Policy
- Safeguarding Policy
- Disciplinary Policy
- Safer Recruitment and Selection Policy

## Procedure/Practice/Guidelines

1. 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.

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 code of practice for the use of surveillance cameras and personal information.

## 2. 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.

**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.

## 3. The data controller

Our school processes personal data relating to parents, students, staff, job applicants, governors, visitors, volunteers and others, and therefore is a data controller.

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

## 4. Roles and responsibilities

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

### 4.1 Local Governing boards

The Local Governing Boards have overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

### 4.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, 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 board their advice and recommendations on school data protection issues.

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

### 4.3 Headteacher

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

**4.4 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 United Kingdom
  - 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

## 5. Data protection principles

The 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.

## 6. Collecting personal data

### 6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **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 effects on them.

### 6.2 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 anonymized. This will be done in accordance with the school's record retention schedule.

## 7. 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 which can provide sufficient guarantees that they comply with data protection law

- o Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- o 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 data protection law.

## 8. Subject access requests and other rights of individuals

### 8.1 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.

### 8.2 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 students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

### 8.3 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.

### 8.4 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 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

## 9. Parental requests to see the educational record

Parents, or those with parental responsibility, who wish to have access to their child's educational record may request this. Requests should be submitted in writing to the school. The school will respond within 15 school days of such 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.

## 10. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students 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 one parent or carer before we take any biometric data from their child and first process it.

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

Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

## 11. CCTV

We use CCTV in various locations around the Trust sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. CCTV footage is recorded and kept for 30 days.

Any enquiries about the CCTV system should be directed to the Headteacher.

## 12. 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 students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

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

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.

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.

## 13. Data protection by design and default

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

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

  - o Appropriate safeguards being put in place if we transfer any personal data outside of the United Kingdom, where different data protection laws will apply
  - o Maintaining records of our processing activities, including:
  - o 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)

## 14. 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 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students 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 ICT Acceptable Usage 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 7)

## 15. 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.

## 16. 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 2. 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 students

## 17. 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.

## Who to contact

The Trust has the responsibility to ensure that your personal data is protected. It is called the **data controller.** All members of staff work for the data controller.

We recommend that you contact the Data Protection Administrator:

Herschel Grammar School
Steven Devereux Email: sde@herschel.slough.sch.uk

Beechwood School
Iain Priestley Email: i.priestley@beechwood.slough.sch.uk

Schools are also required to have someone called a Data Protection Officer or DPO. The DPO advises the school about issues to do with data protection, but can also help you, if you have a problem. Our Data Protection Officer is

Name of DPO: GDPR Sentry Limited
Email address: support@gdprsentry.com
Contact number: 0113 804 2035
Contact address: Unit 434 Birch Park, Thorp Arch Estate, Wetherby, West Yorkshire LS23 7FG

## 18. 2026 legislative and DfE guidance update

### 18.1 Data (Use and Access) Act 2025

The Trust will comply with the Data (Use and Access) Act 2025, which amends and builds on UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations. The Trust will review how personal data is collected, shared and accessed; document the lawful basis used, including any reliance on recognised legitimate interests; review any automated decision-making; maintain staff awareness; and operate a clear, accessible and prompt data protection complaints process.

### 18.2 Data protection complaints

Individuals may raise a complaint about the Trust's handling of personal data with the Data Protection Administrator or DPO using the contact details in this policy. Complaints will be logged, acknowledged, investigated fairly and responded to promptly. The response will explain the outcome, any corrective action, and the individual's right to complain to the Information Commissioner's Office.

### 18.3 Generative artificial intelligence

Staff and pupils must not enter identifiable pupil, parent, carer, staff or other confidential information into a generative AI tool unless the tool has been formally approved for that purpose. Before approval, the Trust will identify the lawful basis, assess data flows and retention, check whether information is used to train the supplier's model, consider international transfers and security, consult the DPO and IT lead, and complete or update a DPIA where processing is likely to present a high risk. AI-generated outputs involving personal data must be checked by an authorised person and must not be used as the sole basis for a significant decision about an individual.

### 18.4 Procuring and monitoring EdTech

The DPO and relevant IT, safeguarding and procurement leads will be involved at the start of any procurement or material change involving EdTech that processes personal data. Due diligence and contracts will address data minimisation, controller and processor roles, sub-processors, security, audit logs, breach notification, support for information rights, international transfers, retention, deletion and return of data, backups and exit arrangements. Non-essential features and additional data collection will be disabled by default. Suppliers and material product changes will be reviewed periodically, and DPIAs and privacy notices updated where processing changes.

### 18.5 Cyber security, filtering and monitoring

The Trust will maintain proportionate technical and organisational measures to protect personal data, including appropriate access controls, multi-factor authentication where available, encryption, patching, backups, logging and arrangements for detecting and responding to incidents. Filtering and monitoring systems used for safeguarding must be configured, accessed and reviewed only by authorised personnel, with clear purposes, proportionate access and retention, and appropriate transparency.

### 18.6 Record keeping and retention

The Trust will maintain a record of processing activities and an approved data retention schedule covering the categories of records it holds, the purpose and lawful basis, responsible owner, retention period or criteria, disposal method and any statutory or safeguarding requirement. Retention will be reviewed regularly. Records subject to a request, complaint, investigation or legal hold must not be altered or destroyed.

### 18.7 Photographs, video, CCTV and biometric systems

Before introducing or materially changing photography, video, CCTV or biometric processing, the Trust will document the purpose, lawful basis, necessity and proportionality, access, security, retention and transparency arrangements, and complete a DPIA where required. For biometric recognition involving children, the Trust will follow the Protection of Freedoms Act 2012 and current DfE guidance, obtain the required written parental consent, respect a child's objection, and provide a reasonable alternative.

### 18.8 Pupil projects and coursework

Where pupils use personal data in projects or coursework, staff must ensure that its use is appropriate, lawful, limited to what is necessary and suitably protected. Wherever practicable, pupils should use anonymised or synthetic information rather than identifiable personal data.

## 19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **at least annually** and shared with the Local Governing Boards.

**Appendix 1: Acceptable use policy for data (AUP)**

All staff and governors should be aware of this agreement, and agree to follow it as a condition of their employment or involvement with the school. Failure to do so may result in disciplinary action.

It is vital that the school fulfils its obligations under the General Data Protection Regulation (2018) and Freedom of Information Act (2000). All staff are given training on this, however this Acceptable Use Policy has been put together to ensure that all staff are aware of and follow specific rules.

### Data to which this AUP applies

1. Sensitive data is any data that could harm, discomfort or embarrass an individual if it were to become public or be made available to an authorised individual. For example SEN, racial or medical data, bank details, phone numbers etc.
2. This AUP also applies to other confidential data such as performance management documents.

### Security of paper-based data

1. Staff are responsible for ensuring that data issued to them remains secure. On site this means keeping data away from being easily accessible by unauthorised personnel e.g. students.
2. If taking data off site, paperwork should be stored securely at all times. You should remain with the data when in transit, and store it in a secure area e.g. a locked cupboard.
3. Particularly sensitive data e.g. SEN or medical records, payroll details etc, should never be removed from the school site and remain in a secure area e.g. locked cupboard, filing cabinet or office at all times.
4. All paper based records containing data should be securely shredded when no longer of use. You should not keep records beyond this time, unless advised otherwise (e.g. child protection records must be kept for longer).

### Security of electronic data

1. Ensure that caution is exercised when logging onto the school's network so that your password cannot be viewed by others.
2. Ensure that you always use your own passwords to log onto the computer system. You never share or use another person's password to log onto the computer system.
3. Ensure you do not log students onto the computer system with your own passwords in order for them to do their own work, browse the internet, watch YouTube during Lunch clubs etc.
4. Ensure that you lock or log out of your computer when leaving it unattended, even for a short period of time. You are responsible for activity that takes place using your credentials, which can be monitored.
5. When storing data in the shared area, ensure that this cannot be accessed by students. Name files appropriately.
6. Ensure that data is not visible to students or other unauthorised personnel. This includes any data in SIMS.net.
7. Data must not be stored on staff laptops or any electronic device outside of school without being encrypted and must comply with the GDPR. In general there should be no need to store data outside of school.
8. Photos and videos of students must only be taken using the school owned devices. Any exception to this can only be authorised by the Headteacher. The placing of photos on websites and social media must be approved by the Headteacher or a member of staff to who this approval has been delegated to by the Headteacher.
9. When deleting a file from a USB drive outside of school you should shift and delete to avoid the risk of a copy of the file being stored in the recycle bin.
10. If you use your mobile device(s) to access school email you must make sure that they are protected with a password or pass-code login. If your device is lost or stolen you must inform the Data Protection Officer or Headteacher as soon as possible.
11. When you leave the school, be aware that your accounts for the network, email and other systems will be disabled when your contract ends. You should ensure that any USB drive issued to you is returned to the IT Department for secure wipe returning it to a re-usable

condition.

12. Upon termination of employment staff should not attempt to copy files from any shared drive or personal area to their own personal external drives. This intellectual data remains the property of Beechwood School.

### Release of data to others

1. Staff may share information with each other regarding students as necessary in the performance of their duties, as long as this sharing of information is in the best interests of the student. The only exception to this is where a manager has explicitly stated that information is not to be shared.
2. When sharing data with another organisation e.g. another school, you should check the legitimacy of the potential recipient. Wherever possible, school to school student data transfers will be made by the data admin staff using the secure B2B and S2S systems. If you are unsure you should consult the Headteacher, and always check before sending data out of the country.
3. Staff with access to data regarding other staff, such as contracts and pay scales, should ensure they have been granted permission to access this data by the Headteacher.
4. You should use your school provided email account for all email related to your work for the school. Your personal email account should never be used.
5. The school takes any data breach very seriously. Should you become aware of any such breach, or the potential for one, you should inform the Headteacher immediately.

### Freedom of Information and Subject Access Requests

1. Any member of staff or the Governing Body may receive a subject access request for personal data, or a request for information under the Freedom of Information Act. Such requests will be made in writing or by email.
2. If you receive such a request, you should inform the Data Protection Officer and Headteacher immediately. The school has a legal duty to respond to requests within a time limit, so it is important that you pass on the request in a timely manner.
3. You should then await a response from the Data Protection Officer or Headteacher before sending a response to the request.
4. Staff should be aware that, in fulfilling requests, the school may be required to disclose the contents of emails. It is therefore vital that staff remain professional in all correspondence.
5. It is an offence to wilfully conceal, damage or destroy information in order to avoid responding to an enquiry, so it is important that no records that are the subject of an enquiry are amended or destroyed.

**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 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 on the school's computer system

  - 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, in clear and plain language, of the nature of the personal data breach

- 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

As above, any decision on whether to contact individuals will be documented by the DPO.

- 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 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 on the school's computer system.

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

### Actions to minimise the impact of data breaches

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

### Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted