



Data Protection Policy

Significant amendments

Author(s)	Assistant Head (Operations) & Bursar
Review body	Safeguarding, Boarding and Health and Safety
Governor approval date	Autumn 2025
Date of review	September 2025
Date of next review	September 2026
Website requirement	Yes
Inspection folder requirement	Yes

Date	Amendment	Initials
01/09/2025	Finalised rewrite based on ISBA guidance	JP

Contents

1. Background	2
2. Definitions	3
3. Application of policy	4
4. The person responsible for data protection at the school	4
5. The principles	4
6. Lawful grounds for data processing	5
7. Headline responsibilities for staff	5
8. Rights of the individual	6
9. Data security online and digital	7
10. Processing of financial/credit card data	7
11. Appendix 1 – personal data breach procedure	8

1. Background

Data protection is an important legal compliance issue for Prestfelde (the “School”). During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notice. The School, as data “controller”, is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the “UK GDPR”) and the Data Protection Act 2018 (“DPA 2018”). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (“ICO”) is responsible for enforcing data protection law in the UK, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

2. Definitions

Term	Definition
Personal data	Any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.
Special categories of personal data	Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.
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 body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.
Data processor	Virtually anything done with personal data, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
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. Application of policy

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties). Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as 'processors' on the School's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party controllers – which may range from other schools, to parents and appropriate authorities – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

4. Person responsible for Data Protection at the School

The School has appointed the Bursar as the Head of Data Protection and Privacy, who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Head of Data Protection and Privacy.

5. The Principles

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers (and processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner.
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for.
3. **Relevant** and **limited** to what is necessary for the purposes it is processed.
4. **Accurate** and kept **up to date**.
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of personal data.

The UK GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- Keeping records of our data processing activities, including by way of logs and policies.
- Documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

6. Lawful grounds for data processing

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under the UK GDPR (and the fact

that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balanced assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as the UK GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7. Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that *any* personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Safeguarding, acceptable use and online safety

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the UK GDPR is on reporting personal data breaches. Controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify Bursar, Richard White. If staff are in any doubt as to whether to report something internally, it is always best to do so.

A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 5 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to Bursar, Richard White, and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to Bursar, Richard White, in the first instance, and at as early a stage as possible.

8. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell Richard White, Bursar as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and

- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must inform Richard White, Bursar as soon as possible.

9. Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

- No member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar.
- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Where a worker is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted.
- Use of personal email accounts or unencrypted personal devices by governors or staff for official School business is not permitted.
- All staff electronic device should be secured by password with two factor identification required where appropriate.

10. Processing of Financial / Credit Card Data

The School complies with the requirements of the PCI Data Security Standard ("PCI DSS"). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard, please seek further guidance from the Bursar. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

Appendix 1: Personal data breach procedure

This procedure is based on guidelines issued by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Head of Data Protection and Privacy (thebursar@prestfelde.co.uk)
- The Head of Data Protection and Privacy will investigate the report, and determine whether a breach has occurred. To decide, the Head of Data Protection and Privacy 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 Head of Data Protection and Privacy will alert the headteacher and the chair of governors
- The Head of Data Protection and Privacy 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 Head of Data Protection and Privacy will assess the potential consequences and impact, based on how serious they are, and how likely they are to happen
- The Head of Data Protection and Privacy 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 Head of Data Protection and Privacy 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 Head of Data Protection and Privacy must notify the ICO.

- The Head of Data Protection and Privacy 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.
- Where the ICO must be notified, the Head of Data Protection and Privacy will do this via the '[report a breach](#)' page of the [ICO website](#) within 72 hours. As required, the Head of Data Protection and Privacy 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 Head of Data Protection and Privacy
 - 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 Head of Data Protection and Privacy 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 Head of Data Protection and Privacy expects to have further information. The Head of Data Protection and Privacy will submit the remaining information as soon as possible
- The Head of Data Protection and Privacy 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 Head of Data Protection and Privacy 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 Head of Data Protection and Privacy
 - 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 Head of Data Protection and Privacy 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 Head of Data Protection and Privacy 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)
 - Any communication taking place with the affected party

Records of all breaches will be stored on the school's computer system.

- The Head of Data Protection and Privacy 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 Head of Data Protection and Privacy as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Head of Data Protection and Privacy will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the Head of Data Protection and Privacy 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 Head of Data Protection and Privacy will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Head of Data Protection and Privacy 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

Non-anonymised pupil exam results or staff pay information being unintentionally shared

- If non-anonymised data is accidentally shared or intentionally shared with inappropriate recipients, the sender must attempt to retrieve the information 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 Head of Data Protection and Privacy as soon as they become aware of the error
- If it is in electronic form and the sender is unavailable or cannot recall the email for any reason, the Head of Data Protection and Privacy will ask the ICT department to recall it
- In any case where the recall is unsuccessful, the Head of Data Protection and Privacy 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
- If it is in hard copy, all originals and copies must be retrieved and the Head of Data Protection and Privacy will ensure we receive a written response from all the individuals who received the data, confirming that they have no other copies
- The Head of Data Protection and Privacy will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Head of Data Protection and Privacy 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

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- If a school device containing non-encrypted sensitive personal data is lost, stolen or hacked the individual who has signed for the device must immediately inform the Head of Data Protection and Privacy. Depending on the circumstances of the loss, the Head of Data Protection and Privacy will inform the police
- If lost, the individual involved must make all attempts to find/retrieve the device before it can be accessed by an unauthorized individual
- The individual responsible must inform the Head of Data Protection and Privacy of all non-encrypted, sensitive personal data which was on the machine at the time of the loss
- If the machine has been hacked, it will be handed over to the ICT department
- The Head of Data Protection and Privacy 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

School or personal mobile phones containing non-encrypted sensitive personal data being stolen or hacked

- Mobile phone data must be protected through a minimum of 6-digit code. Access to school systems should be through two-factor identification.
- If a school or personal phone containing non-encrypted sensitive personal data is lost, stolen or hacked the individual who has signed for the device must immediately inform the Head of Data Protection and Privacy. Depending on the circumstances of the loss, the Head of Data Protection and Privacy will inform the police
- If lost, the individual involved must make all attempts to find/retrieve the device before it can be accessed by an unauthorised individual
- The individual responsible must inform the Head of Data Protection and Privacy of all non-encrypted, sensitive personal data which was on the mobile phone at the time of the loss
- If the device has been hacked, it will be handed over to the ICT department
- The Head of Data Protection and Privacy 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