



PROSPECT HOUSE
SCHOOL

DATA PROTECTION POLICY
SEPTEMBER 2026

1. General Statement of Duties

This policy applies to personal information held and processed by Prospect House School. This policy sets out the school's expectations and procedures with respect to processing any personal data we collect from data subjects (e.g. including parents, pupils and members of staff).

Data protection is an important legal compliance issue for 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, suppliers and other third parties (in a manner more fully detailed in the school's privacy notices). 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 is sensitive or routine.

The data protection framework in the UK consists of the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR), and the Data (Use and Access) Act 2025. All staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

2. The Principles

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- Race
- Ethnic background
- Political opinions
- Religious beliefs
- Trade union membership
- Genetics
- Biometrics (where used for identification)
- Health
- Sex life or orientation

There are also separate rules for the processing of personal data relating to criminal convictions and offences.

The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and has powers to take action for breaches of the law.

The accountability principle requires the school to take responsibility for what it does with personal data and how it complies with the other principles. The school must have appropriate measures and records in place to be able to demonstrate this compliance. This involves among other things:

- Keeping records of data processing activities, including by way of logs and policies
- Documenting significant decisions and assessments about how the school uses personal data

- Generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example, when and how a privacy notice was updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

3. Breaches

Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Accidental breaches may happen (and must be reported: see Section 13 below) and may well not be a disciplinary issue, although the school reserves the right to take disciplinary action for non-compliance with this policy.

4. Key Data Protection Terms

Data controller – an organisation that determines the purpose and means of the processing of personal data. For example, the school is the data controller of pupils' personal information as collected by and processed by the school and its employees. As a data controller, we are responsible for safeguarding the use of personal data.

Data processor – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal information (or personal data) – any information relating to a living individual (a data subject), including name, address, bank details, academic, disciplinary, admissions and attendance records, online identifier such as an email address, health records, race, religion, gender, age, appearance etc. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls and minutes of meetings) is still personal data and regulated by data protection laws, including the UK GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.

Processing – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, disclosing it internally or to third parties, altering it or deleting it. Note that processing can be digital/electronic or manual/physical.

5. Lawful Grounds for Data Processing

Under the UK GDPR there are several different lawful grounds for processing personal data:

Consent: the individual has freely given clear, informed consent for the school to process their personal data for a specific purpose. The definition of what constitutes consent has been tightened under GDPR and this, together with the fact that it can be withdrawn by the data subject, means that the school prefers to rely on another lawful ground where possible.

Legitimate interests: the processing is necessary for the school's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. The school's legitimate interests are set out in their privacy policies.

Contract: the processing is necessary to fulfil a contract with staff or parents.

Legal obligation: including in connection with employment and diversity.

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

6. Data Retention

The school relies on the following lawful reasons for the retention of personal data:

- For the day-to-day running of the school
- In order to comply with the requirements of our insurers (which cover the risk of a future claim from someone who attended the school many years before)
- In order to best be able to defend the school against any claim (including one for historic wrongdoing)
- To examine the history of the school
- To promote the school (for example by showing images of children and staff at the school in the past)

Under UK GDPR principles, schools must not keep personal data for longer than is necessary. Retention periods vary depending on the specific type of record and legal requirements. Personal data about job applicants is retained (and deleted) in accordance with the Recruitment & Recruitment Procedures policy.

If a data subject has any specific queries about how the school's retention policy is applied, or wish to request that personal data is erased, they should contact HR (info@prospecths.org.uk). However, the school will often have lawful and necessary reasons to retain some personal data even following such a request.

7. Staff Responsibilities

Staff should familiarise themselves with the privacy notices for staff, parents and suppliers which are available on the school's website under prospecths.org.uk/privacy.

8. School Data Compliance Officers

Under the UK GDPR, the school is not required to appoint a data protection officer. Instead, the duties of making sure the school is compliant with UK GDPR is the responsibility of the school data compliance officer - Emma Getty. The school data compliance officer has overall responsibility for GDPR compliance and reports to the Head on these issues.

The school's data compliance officer is responsible for:

- Keeping up to date with the UK GDPR and data protection legislation
- Keeping, updating and auditing the personal data ecosystem database
- Keeping, updating and auditing records of external suppliers and as defined by the Data Protection Act 2018 'data processors' and their compliance with UK GDPR
- Liaising with the Head in regard to training, identified risks and any data breach incidents
- Advising the Head and the governors of all significant data protection issues
- Making sure that the staff are aware of data protection requirements
- Ensuring that staff can identify what constitutes a data breach and the workflow of reporting such incidents
- Reporting any potential or actual data breach to the managing director without delay
- Creating best practice guidance for all staff who handle data
- Ensuring that staff use equipment in accordance with the Digital Usage Policy
- Escalating all requests for information by data subjects to the Head
- Managing data protection complaints in accordance with Section 16A of this policy

However, data protection cannot be left to a small handful of individuals in the school: every single member of staff should be aware of how to handle data appropriately and take responsibility for their own actions in doing so.

9. Record-Keeping

9.1 It is important that personal data held by the school is accurate, fair and adequate.

9.2 Individuals are required to inform the school if they believe that their personal data is inaccurate or untrue or if they are dissatisfied with the information in any way. Similarly, it is vital that the way the school records the personal data of others – in particular colleagues, pupils and their parents – is accurate, professional and appropriate.

9.3 Staff should be aware of the rights set out in Section 14 below, whereby any individuals about whom they record information in emails and notes on school business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the school's other policies, and grounds may sometimes exist to withhold these from requests to access personal data. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

10. Data Handling

10.1 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. 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
- Digital Usage

10.2 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.

10.3 Full time teachers and selected administration staff are provided with a device for professional use, e.g., planning or reports. Any other digital equipment may only be taken off site by other staff members with the express permission of the Leadership Team. Requests to do so must be by email. The loan of such equipment will be given on the understanding that any lost, damaged or broken equipment must be paid for by that member of staff. They must also agree to keep any equipment in a private and secure place. A Digital Loan Agreement for such equipment must be completed (accessed in Google Classroom) prior to any such device being taken off site. The device must be returned in person to the IT Department.

11. Care and Data Security

11.1 All school staff are to remain conscious of the data protection principles (see Section 2 above), to attend any training required of them, 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 in terms of handling data. Staff should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

11.2 The school expects all those with management/leadership responsibilities to be particular champions of these principles and to oversee the swift reporting to the Head of any concerns about how

personal information is used by the school, and to identify the need for (and implement) regular staff training.

12. Avoiding, Mitigating, Managing and Reporting Data Breaches

12.1 One of the key obligations contained in the UK GDPR is on reporting personal data breaches.

12.2 The school must notify the ICO if the breach is likely to result in a risk to an individual's rights and freedoms and must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms (see further below). In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO or tell the individuals concerned. If you become aware of a personal data breach you must notify the Head, who must immediately notify the school's governors who is likely to involve one or both of the school data compliance officers. If you are in any doubt as to whether or not you should report something, 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.

12.3 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 other policies.

13. Management of a Personal Data Breach

13.1 A data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The ICO gives the following guidance:

"A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed."

13.2 Data breaches could be caused by a number of factors. For example:

- Loss or theft of pupil or staff data and/or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Poor data destruction procedures
- Human error
- Cyber attack
- Hacking

13.3 Through staff training as referred to in the Digital Usage Policy, staff are trained in identifying data breaches as described above.

13.4 As a data controller, the school is required by law to report a personal data breach to the ICO without undue delay (if it meets the threshold for reporting) and within 72 hours. Depending on the nature of the breach, there could be a fine of up to £17.5m or 4% of the school's annual turnover whichever is greater.

13.5 Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the school must also inform the individual whose data has been the subject of the breach.

13.6 The staff member who identifies a data breach incident or has committed a data breach must report the incident to the Head who must report it immediately to the school's governors.

13.7 The notification referred to in 13.6 shall at least:

- Describe the nature of the breach including where possible, the categories and approximate number of personal data records concerned
- Describe the likely consequences of the personal data breach
- Describe the measures taken and measures proposed to address the breach

Where this information is not yet available, the report should provide as much information as possible with further information to follow as it becomes available.

13.8 The school's governors will likely involve the school data compliance officers, as is considered appropriate, to determine the appropriate actions in response to the breach and to ensure such actions are carried out, including, if appropriate, any reporting necessary.

13.9 In the event of a suspected personal data breach, the following procedure should be followed:

Step 1: The person who discovers/receives a report of a breach must inform the Head or, in their absence, the Deputy Head. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

Step 2: The Head should notify the school's governors immediately. If they are not immediately available, the Head should also notify the school data compliance officers who should contact the chairman. Steps must be taken as soon as possible to minimise the effect of the breach. An example might be to shut down a system.

Step 3: As a registered data controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

Step 4: The school's governors must also consider whether the police need to be informed. This might be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

Step 5: The school's governors together with the school data compliance officer(s) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

- Attempting to recover lost equipment
- The use of back-ups to restore lost/damaged/stolen data
- If the data breach includes any entry codes or IT system passwords, changing these immediately and informing the relevant agencies and members of staff

Step 6: In most cases, the next stage would be for the school's governors (or such person as they appoint) to investigate the breach. The school's governors should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data
- Its sensitivity
- What protections were in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach

Step 7: The school's governors must determine whether the breach is such that it must be reported to the ICO and/or to the data subject(s) concerned and, where it is considered that there is an obligation to report, ensure that such reports are made. Where the school's governors determine that no such report is required, their reasons for concluding must be recorded on the breach log.

Step 8: A clear record should be made of the nature of the breach, the actions taken to mitigate it, whether it triggered any reporting obligations, if so, on what date it was reported and if not, why not. This should be done by the school's governors or by a school data compliance officer on the 'Breaches' section of the relevant school's GDPR account. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the ICO. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the immediate issue has been resolved.

Step 9: Once the initial aftermath of the breach is over, the school's governors should fully review both the causes of the breach and the effectiveness of the response to it. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

14. Rights of Individuals

14.1 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 data 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 an individual becomes aware of a subject access request (or indeed any communication from an individual about their personal data), the individual must inform the Head by email as soon as possible, who must then report it to the managing director.

14.2 Individuals also have legal rights to:

- Require the school to correct the personal data it holds about them if it is inaccurate
- Request that the school erases their personal data (in certain circumstances)
- Request that the school restricts its data processing activities (in certain circumstances)
- Receive from the school the personal data it holds about them for the purpose of transmitting it in a commonly used format to another data controller
- Object, on grounds relating to their particular situation, to any of the school's particular processing activities where the individual feels this has a disproportionate impact on them
- Object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where the school is relying on it for processing their personal data

14.3 Except for the final bullet point, none of these rights for individuals is unqualified and exceptions may well apply. In any event, however, if a member of staff receives a request from an individual who is purporting to exercise one or more of their data protection rights, they must email the Head to inform them as soon as possible.

15. Processing of Credit Card Data

The school complies with the requirements of the Payment Card Industry 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 Finance Officer.

16. Complaints to the ICO

If an individual believes that the school has not complied with this policy or not acted in accordance with data protection legislation, and they remain dissatisfied after following the school's data protection complaints procedure (see Section 16A below), they may make representations to the Information Commissioner by calling the helpline on 0303 123 1113 or log a complaint on the ICO website <https://ico.org.uk/make-a-complaint/>

16A. Data Protection Complaints Procedure

16A.1 What is a Data Protection Complaint?

People can complain to the school if they believe we haven't correctly followed data protection legislation in the way we've handled their personal information (or the personal information of someone they're acting on behalf of).

For example, a pupil or parent could complain about:

- The way we've responded to their subject access request (SAR)
- The security measures we've used to protect their information
- How we've collected or used their personal information

To complain, they don't have to use legal terms or quote sections of the legislation. If we're not sure if someone is making a data protection complaint, we will ask them to clarify so we can make sure we're following the right procedures.

16A.2 How to Make a Data Protection Complaint

Individuals can make data protection complaints to the school via:

- Email: info@prospecths.org.uk (marked for the attention of Emma Getty)
- Written letter: Addressed to Emma Getty, Prospect House School, 75 Putney Hill, London, SW15 3NT
- Telephone: 0208 780 0456 and ask to speak to a member of the Senior Leadership Team
- In Person: By speaking to a member of the senior leadership team

There is no obligation for complainants to use these specific methods of contact. People can complain in any way they choose and we will accept the complaint.

All data protection complaints should be directed to Emma Getty (School Data Compliance Officer) in the first instance.

16A.3 Information in Privacy Notices

Our privacy notices (available at prospecths.org.uk/privacy) inform individuals that they can make data protection complaints to the school and provide the contact details set out above. The privacy notices also inform individuals of their right to complain to the Information Commissioner's Office if they are dissatisfied with our response.

When we respond to subject access requests, we also inform individuals of their right to complain about how we've handled their personal data.

16A.4 Acknowledging Complaints

We will acknowledge all data protection complaints within 30 days of receipt.

The 30-day period begins the day after we receive the complaint. It doesn't matter if this day falls on a weekend or a public holiday – the 30 days will always start on this day. If the last day to acknowledge the complaint falls on a weekend or public holiday, we have until the next working day to provide an acknowledgement.

Our acknowledgement will:

- Confirm we've received the complaint
- Confirm that we will investigate the matter
- Provide a point of contact for any questions
- Where possible, provide an indication of when the complainant can expect to receive an outcome

We will generally respond in the same way we received the complaint. For example:

- If the complaint is via email, we will reply via email
- If the complaint is in writing, we will send an acknowledgement letter
- If the complaint is verbal (e.g. over the phone or face-to-face), we will acknowledge this verbally and follow up in writing

If the complaint is made via social media, we will ask for an alternative contact method instead, as this is not a secure way of communicating.

16A.5 Identity Verification

If we have any doubts about the complainant's identity, we will ask them for proof of ID at the earliest opportunity before we respond. If we have enough information to be sure about the complainant's identity, we will not ask for more.

Acceptable forms of ID include:

- Passport
- Driving licence
- Utility bill (dated within the last 3 months)
- Birth certificate (for pupils)

16A.6 Complaints Made on Behalf of Others

We may receive a complaint on behalf of another person (known as a third party). For example, a family member or solicitor.

If so, we will check that the third party is authorised to act on the other person's behalf. The form of evidence we need depends on the circumstances, but some examples are:

- An appropriate power of attorney
- A signed letter of authority from the person they are acting on behalf of

If we have no evidence that a third party is authorised to act on someone's behalf, we will not investigate the complaint until we receive the appropriate authority.

16A.7 Complaints from Parents About Their Child's Data

Under data protection law, parents don't have an automatic right to exercise the rights of their child. We will only allow parents to make a complaint on behalf of their child if:

- The child authorises them to do so; or
- The child does not have sufficient understanding to exercise the rights themselves; or
- It is clear that this is in the best interests of the child

We will assess each case individually, taking into account the age and maturity of the child and the nature of the complaint.

16A.8 Complaints from Pupils

Children have the same rights over their personal information as adults. However, we will assess the competence of the child to understand and exercise their rights.

If we receive complaints from pupils, we will respond in plain, clear language they can understand.

16A.9 Investigating the Complaint

Our investigation will begin immediately upon receipt of the complaint. We will investigate the complaint without undue delay, which means we will look into the issue as soon as possible.

We will start by:

- Looking at all the relevant facts thoroughly, fairly and accurately
- Speaking to relevant members of staff
- Comparing the information from the complaint with the information we hold
- Checking we've upheld our own terms, policies and standards

If we aren't sure what the complaint is about, we will ask the person making it for more information as quickly as possible. We will also ask what outcome they're looking for. For example, they might want us to change a decision we've made, apologise for a mistake, or change our processes.

The amount of time we spend on the investigation will depend on the scale and complexity of the issue. We will:

- Make an appropriate level of enquiries based on the circumstances of each complaint
- Be able to justify why we handled a complaint in the way we did

The important thing is to consider each complaint on a case-by-case basis, not to apply a set period of time as a blanket approach.

Note: The 30-day time limit applies to acknowledging the complaint, not investigating and providing an outcome. A complex complaint may take longer than 30 days to investigate, but we must be able to justify why this delay is necessary.

16A.10 Keeping the Complainant Informed

We will keep the person making the complaint updated on the progress of the investigation without undue delay. This means keeping them up to date with timeframes and explaining any delays. We don't need to tell them what steps we've taken so far.

For example, if the investigation is likely to take some time, we will follow up on our initial response so the complainant knows we're working on it. We will provide them with a date for when we expect to finish our investigation and a point of contact for any questions.

16A.11 Providing an Outcome

When we've completed our investigation, we will let the complainant know the outcome as soon as possible (without 'undue delay').

If we're able to investigate the complaint and provide an outcome within 30 days, we're not required to provide an acknowledgement and outcome separately. However, to maintain good relationships we will acknowledge the complaint as soon as possible, so the complainant feels reassured that we're looking into it.

When we share the outcome, we will:

- Explain what we've done to resolve the complaint and, where appropriate, any actions we've taken as a result
- If we think that we've complied with data protection law, explain this in detail to the complainant
- Provide enough information to help the complainant understand how we've reached our conclusion
- Remind the complainant of their right to complain to the Information Commissioner's Office if they remain dissatisfied

16A.12 Record-Keeping

For each data protection complaint we receive, we will keep a record of:

- The date we received it
- Our acknowledgement
- Any relevant conversations and documents
- The outcome of the complaint
- Any actions we took as a result of our investigation

We will retain these records in line with our data retention schedule.

Emma Getty will maintain a data protection complaints log to track:

- The number of data protection complaints we receive
- Any recurring themes
- Areas for improvement

This will help us identify potential compliance issues and improve our data protection practices.

16A.13 Review and Learning

Once we've provided an outcome, we will review what happened and consider if there's anything we can learn or improve to prevent future complaints.

Emma Getty will report to the Head and governors on:

- The number and nature of data protection complaints received
- Any trends or patterns identified
- Recommendations for improvements to policies, procedures or training

16A.14 Right to Complain to the ICO

If complainants are dissatisfied with our response, they may complain to the Information Commissioner's Office by:

- Calling the helpline on 0303 123 1113
- Logging a complaint on the ICO website: <https://ico.org.uk/make-a-complaint/>

We will inform complainants of this right in our acknowledgement and in our final response.

17. Note on the Freedom of Information Act 2000

The operation of the Freedom of Information Act 2000 is confined to the public sector and therefore has no application to independent schools.

