PROSPECT HOUSE

SCHOOL

DATA PROTECTION POLICY
(and NOTES ON THE FREEDOM OF INFORMATION ACT 2000)

September 2023

DATA PROTECTION POLICY

1. General statement of the duties within Prospect House School

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 Act 2018 controls how personal information is used by organisations, businesses or the government. The Data Protection Act 2018 (DPA 2018) is the UK's implementation of the General Data Protection Regulation (GDPR). 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'. she/he 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:

1. keeping records of data processing activities, including by way of logs and policies;
2. documenting significant decisions and assessments about how the school uses personal data; and
3. 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 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 used in this data protection policy are:

- 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 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 GDPR there are several different lawful grounds for processing personal data:

a. 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;

b. 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;

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

d. Legal obligation including in connection with employment and diversity;

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

f. 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:

1. for the day-to-day running of the school
2. 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)
3. in order to best be able to defend the school against any claim (including one for historic wrongdoing)
4. to examine the history of the school
5. to promote the school (for example by showing images of children and staff at the school in the past)

The school aims to retain pupil and staff personal data for 50 years. 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, he or she 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 GDPR, the school is not required to appoint a data protection officer. Instead, the duties of making sure the school is compliant with GDPR ais the responsibility of the school data compliance officer - Head of Computing. The school data compliance officer has overall responsibility for GDPR compliance reports to the Head on these issues.

The school's data compliance officer is responsible for:

a) Keeping up to date with the GDPR
b) Keeping, updating and auditing the personal data ecosystem database
c) Keeping, updating and auditing records of external suppliers and as defined by the Data Protection Act 2018 'data processors' and their compliance with GDPR
d) Liaising with the Head in regard to training, identified risks and any data breach incidents
e) Advising the Head and the Givernor of all significant data protection issues
f) Making sure that the staff are aware of data protection requirements
g) Ensuring that staff can identify what constitutes a data breach and the workflow of reporting such incidents
h) Reporting any potential or actual data breach to the managing director without delay
i) Creating best practice guidance for all staff who handle data
j) Ensuring that staff use equipment in accordance with the Digital Usage Policy
k) Escalating all requests for information by data subjects to the Head

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 she/he believes that their personal data is inaccurate or untrue or if she/he is 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 below, whereby any individuals about whom she/he records 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 she/he comes into contact with fairly, lawfully, responsibly and securely and in accordance with the 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 Fulltime 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 offsite by other staff members with the express permission of the Head of computing. Requests to do so must be by email to the Head of computing. 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. she/he 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 offsite. The device must be returned in person to the Head of computing on its return.

11. Care and data security

11.1 All school staff are to remain conscious of the data protection principles (see above), to attend any training required of them, and to use their best efforts to comply with those principles whenever she/he processes 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 identity the need for (and implement) regular staff training.

12. Avoiding, mitigating, managing and reporting data breaches

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

12.2 Data 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 Governor 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:

a) Loss or theft of pupil or staff data and/or equipment on which data is stored
b) Inappropriate access controls allowing unauthorised use
c) Equipment failure
d) Poor data destruction procedures
e) Human error
f) Cyber attack
g) 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 schools 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 Governor.

13.7 The notification referred to in 13.6 shall at least:

a) describe the nature of the breach including where possible, the categories and approximate number of personal data records concerned.
b) describe the likely consequences of the personal data breach
c) 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 Governor 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:

a) 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.

b) The Head should notify the school's Governor immediately. If she/he is 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.

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

d) The school's Governor 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.

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

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

f) In most cases, the next stage would be for the school's Governor (or such person as she/he appoints) to investigate the breach. The school's Governor 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.

g) The school's Governor 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 Governor determines that no such report is required, their reasons for so concluding must be recorded on the breach log.

h) 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 a the school's Governor or by a school data compliance officer on the 'Breaches' section of the relevant school's GDPRiS 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.

i) Once the initial aftermath of the breach is over, the school's Governor 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; and
- 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, he or she must email the head to inform him/her 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 she/he 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 Ofiicer.

16. Complaints

If an individual believes that the school has not complied with this policy or not acted in accordance with the GDPR he/she should utilise the school's complaints procedure.

If the individual is still not satisfied, he/she may make representations to the Information Commissioner by calling the helpdesk on 0303 123 1113 or log a complaint on the ICO website https://ico.org.uk/make-a-complaint/

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.