PARKSIDE HOUSE SCHOOL

Data Protection Policy

School Year 2017 – 2018

Contents

1. Introduction

Parkside House school regards the lawful and correct processing of personal and sensitive data as an integral part of its purpose and vital for maintaining confidence between employees, clients and others whom we process data about, on behalf of and ourselves.

2. Policy Statement

This Data Protection Policy explains how the school will meet its legal obligations concerning confidentiality and data security standards. The requirements within the policy are primarily based upon the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) (the Legislation) which cover data security and confidentiality of personal and sensitive personal data. (A list of important defined terms in the GDPR can be found on the back pages of this policy).

- PHS will fully implement all aspects of the Legislation.
- PHS will ensure all employees and others handling personal data are aware of their obligations and rights under the Legislation.
- PHS will implement adequate and appropriate physical, technical and organisational measures to ensure the security of all data contained in or handled by those systems.

The main focus of this policy is to provide guidance about the protection, sharing and disclosure of employee and client data, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to anyone handling personal data or sensitive (to be called "Special Category" in the GDPR) data on behalf of school.

3. Registration with the Information Commissioner

3.1 GDPR requires data controllers (to register with the Information Commissioner (ICO) the categories of personal data they hold, and what they do with it.

3.2 PHS is registered with the ICO.

3.3 PHS is a "data controller" when it decides how to use personal data. It is a "data processor" when it is directed by a third party as to how to use personal data. Further to the GDPR both data controllers and data processors have legal obligations to safeguard personal data and are both liable if there is a breach.

4. Definitions of Personal Data and Sensitive Personal Data

- Personal data is any personally identifiable information, so this includes:
  - employee data
  - client data
  - Any other personal data processed by PHS

4.1 Examples of personal data which PHS processes include:

- Names, addresses, emails, phone numbers and other contact information;
- Financial information;
- National insurance numbers and payroll data;
  CCTV images and photographs, video and audio recordings.

4.2 Certain types of data are identified as sensitive or "special category" and attract additional legal protection. Sensitive personal data is any data that could identify a person together with information about their:

- racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Membership of a trade union;
- Physical or mental health or condition;
- Sexual life;
- Commission or alleged commission of any offence;
- Information about any proceedings for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of a court in such proceedings.
  .

5. Data Protection Principles

5.1 We must all comply with the six Data Protection principles that lie at the heart of the Legislation. The school fully endorses and abides by the data protection principles. Specifically, the six principles require that data is:

- **Principle 1:** Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').

- **Principle 2:** Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation').
- **Principle 3:** Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

- **Principle 4:** Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

- **Principle 5:** Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation') (see our Retention Policy).

- **Principle 6:** Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5.2 Personal data and sensitive personal data must not be used other than for specific purposes. The data subject should always know that their data is being processed and the purpose. This information is provided in our Privacy Policies. When that data is sensitive, for example health information, consent is required before the data can be processed by PHS.

5.3 All data collected from young people under the age of 16 (unless there are concerns about mental capacity in which case this should be extended), is not classed as sensitive personal data but should be treated as sensitive personal data.

5.4 A record incorporating personal data can be in computerised and/or manual form. It may include such documentation as:

- Manually stored paper data e.g. employee records.
- Hand written notes.
- Letters to and from PHS.
- Electronic records.
- Printouts.
- Photographs.
- Videos and tape recordings.

5.5 Backup data (i.e. archived data or disaster recovery records) is also subject to the Legislation. A search in backup data should only be conducted if specifically asked for by the data subject.

6. Rights of Individuals

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object to processing.
- Rights in relation to automated decision making and profiling.

7. The Right of Access

The Legislation gives every living person (or their authorised representative) the right to apply for access to the personal data which organisations hold about them irrespective of when and how they were compiled, i.e. hand written records, electronic and manual records held in a structured file, subject to certain exemptions. This is called a Subject Access Request. The Legislation treats personnel data relating to employees and clients alike.

8. Retention Periods

We store personal data on secure servers in accordance with the criteria set out in our Data Retention Policy.

9. Practical Implications

9.1 Understanding and complying with the principles is the key to understanding and complying with our responsibilities as a data controller. Therefore, PHS will, through appropriate management, and strict application of criteria and controls:

- Ensure that there is a lawful basis for using personal data.
- Ensure that the use of the data is fair and will meet one of the specified conditions.
- Only process sensitive personal data where PHS has obtained the individual's explicit consent; unless an exemption applies.
- Only process sensitive personal data, if it is absolutely necessary for PHS to use it.
- Explain to individuals, at the time their personal data is collected, how that information will be used (within our Privacy Policies).
- Only obtain and use personal data for those purposes which are known to the individual.
- Only process personal data for the purpose for which it was given. If we need to use the data for other purposes, further consent may be needed.
- Only keep personal data that is relevant toPHS.
- Keep personal data accurate and up to date.
- Only keep personal data for as long as is necessary (see our Retention Policy).
- Always adhere to our Subject Access Request Procedure and be receptive to any queries, requests or complaints made by individuals in connection with their personal data.
- Always allow individuals to opt-out of receiving bulk information with exception of core administrative emails such as renewals. The school will always suppress the details of individuals who have opted out of receiving information (e.g. marketing).

- Will always give an option to “opt in” when consent is needed to process personal data unless there is a statutory/ legal exemption.
- Take appropriate technical and organisational security measures to safeguard personal data.

9.2 In addition, PHS will ensure that:

- There is an employee appointed as the Data Protection Officer with specific responsibility for Data Protection in PHS (see below for roles and responsibilities).
- Everyone managing and handling personal data and sensitive personal data understands that they are legally responsible for following good data protection practice and has read and signed the policy.
- Everyone managing and handling personal data and sensitive personal data is appropriately supervised by their line manager.
- Enquiries about handling personal data and sensitive personal data are promptly and courteously dealt with.
- Methods of handling personal data and sensitive personal data are clearly described in polices and guidance.
- A review and audit of data protection arrangements is undertaken annually.
- Methods of handling personal data and sensitive personal data are regularly assessed and evaluated by the Data Protection Officer and relevant directors.
- Performance with personal data and sensitive personal data handling is regularly assessed and evaluated by the Data Protection Officer and relevant directors.
- Formal written data processing agreements are in place before any personal data and sensitive personal data is transferred to a third party.

10. Roles and Responsibilities

10.1 Maintaining confidentiality and adhering to Data Protection Legislation applies to everyone at PHS. The School will take necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice. Employees will receive training and sign this policy every twelve months as part of their induction.

10.2 All employees [**and volunteers**] and sub-contractors/associates have a responsibility to:

- Observe all guidance and codes of conduct in relation to obtaining, using and disclosing personal data and sensitive personal data;
- Obtain and process personal data and sensitive personal data only for specified purposes;
- Only access personal data and sensitive personal data that is specifically required to carry out their activity or work;
- Record data correctly in both manual and electronic records;
- Ensure any personal data and sensitive personal data held is kept secure;
- Ensure that personal data and sensitive personal data is not disclosed in any form to any unauthorised third party;
- Ensure personal data and sensitive personal data is sent securely; and
- Read and sign this policy, raising any questions to check understanding.

10.3

10.4 All Senior Leaders are responsible for:

- Determining if their operational area holds personal data and sensitive personal data and ensuring that the data is adequately secure, access is controlled and that the data is only used for the intended purposes(s);
- Providing clear instructions to their teams about data protection requirements and measures;
- Ensuring personal and sensitive personal data is only held for the purpose intended;
- Ensuring personal and sensitive personal data is not communicated or shared for non authorised purposes; and
- Ensuring personal and sensitive personal data is encrypted when transmitted or appropriate security measures are taken to protect when in transit or storage.

10.5 Our Data Protection Officer is Jackie Burton. Responsibilities include:

- Ensuring compliance with legislation principles;
- Progressing the Data Protection Action Plan;
- Providing guidance and advice to employees in relation to compliance with legislative requirements;
- Auditing data protection arrangements continually;
- Reporting on any breaches of Data Protection Legislation;
- In the Data Protection Officer's absence, advice can be gained from Belinda Young and general information can be found at http://www.ico.gov.uk/; and
- Ensuring those handling personal data are aware of their obligations by producing relevant policy, auditing the arrangements and ensuring relevant people receive training.

10.6 Responsibility of the Head Teacher. The Headteacher has overall responsibility for data protection within the school. The school has a duty to ensure that the requirements of the Legislation are upheld. PHS relies on each of its employees and sub-contractors/associates to help in ensuring secure systems are in place to protect personal data. Please let us know if you see or foresee any problems.

10.7 The Information Commissioner Office (ICO) – The Information Commissioner's Office is responsible for overseeing compliance e.g. investigating complaints, issuing codes of practice and guidance, maintaining a register of data protection officers. Any failure to comply with the Legislation may lead to an investigation by the ICO which could result in serious financial or other consequences for the school.

11. Breach of Policy

In the event that we fail to comply with the Legislation, an individual can complain to the DPO and/or ICO. We respectfully request that you notify the DPO or Jackie Burton in any event.

12. Dealing with a Data Breach

12.1 If a data breach is anticipated or identified, the person who identifies the actual or potential breach should immediately contact the DPO who will inform the ICO within 72 hours:

- Notify the relevant department manager by telephone or in person
- Notify the Data Protection Officer by telephone or in person
- Complete and return a breach report available from the Data Protection Officer.

This must be done whether the breach is identified inside or outside working hours. For out of hours breach reporting contact Belinda Young

12.2 Following notification of a breach, the Data Protection Officer will take the following actions as a matter of urgency:

- Implement a recovery plan, including damage limitation;
- Assess the risks associated with the breach;
- Inform the appropriate people and organisations that the breach has occurred;
- Review our response and update our information security.

13. Policies and Procedures

This policy should be read in conjunction with the following policies and guidance:

Policies:

- Data Handling Procedure
- The GDPR Privacy Policy

Guidance:

- Document Encryption Guidance
- Dealing with a Data Subject Access Request
- The 'Conditions of Processing'

Signed on behalf of PHS:

Date: June 2018

Print Name: Belinda Young

Glossary of Terms

Consent
Clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written (including electronic) statement.

Data Subject
Means an individual who is the subject of personal data or sensitive personal data. This includes an employee, client or other identifiable individual.

Data Controller
Means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data and sensitive personal data are, or are to be processed.

The data controller is PHS for employee data.

Data Processor
In relation to personal data or sensitive personal data, means any person who processes that data on behalf of the data controller but is not employed by them. PHS is a data processor in respect of pupil data.

Third Party
In relation to personal data or sensitive personal data, means a natural or legal person other than the data subject, the data controller, or any data processor or other person authorised to process data for data controller or processor. For example, the police or HMRC.

Personal Data
Any information relating to an identified or identifiable natural person ('data subject'): an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

Processing
Means recording or holding data or carrying out any operations on that data; including organising, altering or adapting it; disclosing the data or aligning, combining, blocking or erasing it. Essentially if you have it, you are processing it.

Data Breach
Is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or sensitive personal data transmitted, stored or otherwise processed.

Subject Access Request
This is a written, signed request (which includes emails and other written formats) from an individual to see data held on them. The Data Controller must provide all such information in a readable form within 30 days of receipt of the request.