DEVONPORT HIGH SCHOOL FOR GIRLS

DATA PROTECTION POLICY

Named person: Mrs Anita Hemsi

Category: Statutory

Review: Bi-Annually

Date to be reviewed: Spring 2020

This policy has been reviewed with regard to the work/life balance of staff.

Ratified at the Full Governors' meeting on: 21/05/18

DEVONPORT HIGH SCHOOL FOR GIRLS
DATA PROTECTION POLICY

Devonport High School for Girls collects and uses personal information (referred to in the Data Protection Act as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is registered as a Data controller, with the Information Commissioner's Office (ICO). Details are available on the ICO website.

Purpose

This policy sets out how the school deals with personal information correctly and security in accordance with the Data Protection Act 1998, and other related legislation. The Data Protection Act 1998 is superseded by the introduction of the General Data Protection Regulations which become effective on 25th May 2018. These regulations will eventually be consolidated within UK Law by a revised Data Protection Bill. However, during the BREXIT transition, GDPR will apply fully to the UK. GDPR aims to harmonise personal data security across the EU as well as providing new subject rights which more properly reflect the advent of social media and the growth of the internet.

This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.

All school staff and governors involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

What is Personal Information or data?

Personal information or data is information which relates to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The regulations state that 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 number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Please see Appendix A Privacy Notice for our Pupils and Appendix B Privacy Notice for Employees, Agency Workers, Governors and Trustees. Current versions of these documents are available on the school website.

Responsibilities under GDPR

Devonport High School for Girls Academy Trust will be the "data controller" under the terms of the regulations – this means it is ultimately responsible for controlling the use and processing of the personal data.

The Head Teacher is responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging transparent, proportionate, and secure data and information handling within the school.

The Head Teacher is also responsible for ensuring that the school's notification is kept accurate. Details of the school's notification can be found on the Office of the Information Commissioner's (ICO) website (www.informationcommissioner.gov.uk).

Compliance with GDPR is the personal responsibility of all members of the school who process personal data. Individuals who provide personal data to the school are responsible for ensuring that the information is accurate and up-to-date.

Lawful Basis for processing information under GDPR

There are 6 lawful bases for processing personal data:

1. Consent – which should be expressed, not implied, and should be easily understood
2. Performance of a contract
3. Legal compliance – necessary to comply with the law
4. Protection of vital interests – necessary to protect someone's life
5. Public task
6. Legitimate interests

For DHSG students, the lawful bases will generally be legal compliance and performance of a public task. Where specific consent is sought, the school will ensure that any forms used to gather data on an individual will contain a Fair Collection Statement explaining the use of that data and how the data may be disclosed.

For DHSG staff, the lawful basis will be the performance of a contract.

Data Protection Officer

Under GDPR the school is bound to appoint a Data Protection Officer, who will perform an advisory role in helping the school to exercise its responsibilities under the GDPR regulations. The Business Manager has been appointed to this role.

Data Protection Principles

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definition of personal and sensitive data shall be those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

The principles of GDPR shall be adhered to at all times for all data processed:

- Personal data should be processed fairly, lawfully and in a transparent manner.

- Data should be obtained for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes.
- The data should be adequate, relevant and not excessive
- The data should be accurate and where necessary kept up to date
- Data should not be kept for longer than necessary
- Data should be kept secure

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the school, including information held within their educational record. Requests for information must be made in writing (this includes email) and addressed to the Head Teacher. Any member of staff receiving a Subject Access Request (SAR) should forward this to the Head Teacher. If the initial request does not clearly identify the information required then we may ask for clarification. When making a request, the school can request evidence of identity such as a passport, driving licence or utility bill.

Information must be provided free of charge; however, a "reasonable fee" may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. A charge may also be made to comply with requests for further copies of the same information.

The school will respond to requests within 1 month (irrespective of school holidays). However, the 1 month deadline will not commence until receipt of fees or clarification of information has been sought.

Commitment

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why personal information is being collected.
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (Subject Access Requests).
- Ensure all staff and governors are aware of and understand these policies and procedures.

Disclosure of Data

The school undertakes not to disclose personal data to unauthorised third parties, including family members, friends, social networking groups and government bodies.

Legitimate disclosure may occur in the following instances:

- The individual has given their consent to the disclosure

- The disclosure has been notified to the Information Commissioner's Office and is in the legitimate interests of the school
- The school is legally obliged to disclose the information
- The disclosure is required for the performance of a contract

Derogation

EU Member states can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- National security
- Defence
- Public Security
- The prevention, investigation, detection or prosecution of criminal offences
- Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security
- The protection of judicial independence and proceedings
- Breaches of ethics in regulated professions
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, or other public interests or crime/ethics prevention
- The protection of the individual, or the rights and freedoms of others
- The enforcement of civil law matters

Data Security

In order to assure the protection of all data being processed, the school will continue to monitor and evaluate risks associated with maintaining and processing personal data. Security of data shall be achieved through the implementation of proportionate physical and technical measures. The security arrangements of any organisations with which data are shared shall also be monitored and these organisations will be asked to provide evidence of their competence in the security of shared data.

Data Retention and Disposal

Data will be retained and either securely disposed of or archived in accordance with the guidelines specified at Appendix A.

Data Breach

GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO). Where feasible this needs to be done within 72 hours of becoming aware of the breach.

When a personal data breach has occurred, the school will establish the likelihood and severity of the resulting risk to individual rights and freedoms. Where it is determined that there is a risk, the school will report to the ICO and the affected individuals will be informed without undue delay.

Full records will be kept of any personal data breaches, regardless of whether notification to the supervising authority is required.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or at www.ico.org.uk.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years.