PLYMOUTH HIGH SCHOOL FOR GIRLS

POLICY: DATA PROTECTION POLICY

SLT LINK MEMBER:	**Shaun Willis**
GOVERNORS SUB COMMITTEE:	**P & R**
This policy was adopted/updated:	May 2018
This policy will be reviewed:	September 2020
Statutory Policy:	NO
Source:	LA/School

Contents

DATA PROTECTION POLICY

Plymouth High School for Girls

1.0 INTENTIONS

Plymouth High School for Girls supports the objectives of the Data Protection Act 2018 (DPA 2018) and intends to conform to the requirements of the Act at all times.

The DPA 2018 sets out six data protection principles that our school is responsible for and must be able to demonstrate compliance with. This policy details how the school will comply with these principles.

2.0 LEGISLATION AND GUIDANCE

The DPA 2018 makes provision for dealing with personal data. Most processing of personal data is subject to the General Data Protection Regulations (GDPR) which describes how personal information must be managed. The GDPR recognises changes in technology and the way organisations collect information. The DPA applies to all personal data regardless of the format in which it is collected or stored.

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. The Information Commissioner's Office has responsibility for monitoring and enforcing the provisions of the GDPR and DPA 2018.

3.0 OUR SCHOOL'S ROLES AND RESPONSIBILITIES

This policy must be complied with fully by all Governors, staff, volunteers, contractors and suppliers of Plymouth High School for Girls who collect, hold, process or deal with Personal Data for or on behalf of the school. Employees who do not comply with this policy may face disciplinary action.

3.1 Governing Board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

3.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Plymouth City Council's DPO is:
Liz Easterbrook
Data Protection Officer
Finance
Plymouth City Council
Ballard house
West Hoe Road
Plymouth
PL1 3BJ
Email: dataprotectionofficer@plymouth.gov.uk
Tel: 01752 398380

Plymouth High School's DPO is:
Kathryn Rogers
Data Protection Officer
Plymouth High School
St Lawrence Road
Plymouth
PL4 6HT
Email: phs@phsg.org
Tel: 01752 208308

3.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

3.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy and any supporting policies and processes implemented by the school.
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO:
    - With any questions about the application of this policy, data protection law, retaining personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If there has been a definite or suspected data breach or if there has been a 'near miss';
    - If they are unsure whether or not they have a lawful basis to collect or process personal data for a particular reason;
    - If they receive a data protection rights requests from an individual;
    - If they need to rely on or capture consent, outside of the existing consent requirements of the school or if they need to draft a privacy notice;
    - Transfer personal data outside the European Economic Area or use any third party that intends to do so;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they need help with any contracts or sharing personal data with third parties;

4.0 DEFINITIONS

4.1 The following table provides a list of important terms and their meanings for the purposes of this data protection policy.

TERM	DESCRIPTION
Data Subject	The identified or identifiable individual that the personal data being held or processed relates to.
Personal data	Information relating to a natural identifiable person, whether directly or indirectly.
Special category data	These are highly sensitive pieces of information about people. They are important because under GDPR they are afforded extra protection in terms of the reasons we need to have to access and process that information. This is defined as data relating to: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Health - physical or mental • Trade union membership • Sex life or sexual orientation • Data relating to criminal offences is also afforded similar special protection. In education we also apply this special protection to other categories of personal data which is considered to be highly sensitive, such as: • Free school meals • Pupil premium eligibility • Special educational needs • Children in need/children looked after • Children Services Interactions • Safeguarding
Processing	This includes anything that is done with personal data such as collecting, recording, storing, organising, structuring, adapting, altering, retrieving, using, sharing, erasing or destroying. Processing can be automated or manual.
Data Controller	The organisation who (either alone or in common with other people or organisations) determine the purpose for which, and the manner in which data are processed.
Data Processor	A person or organisation who process data on behalf of and on the orders of a controller.
Data audit/data asset register	The assessment of data and its quality, for a specific purpose.
Lawful basis and	These are the specific reasons, set out in law, for which we can process

conditions for processing	personal data. There is one list for personal data (lawful basis article 6) and another list for processing special category data (article 9).
Data retention	How long we will hold information to carry out the processing job we need it for. At the end of a data retention period, personal data will be disposed of securely.
Subject Access Request (SAR)	This is where a data subject requests access to the information we hold about them.
Data Protection Impact Assessment (DPIA)	This is a process to consider the implication of a change we are introducing on the privacy of individuals' data, for example if we are introducing a new system.
Data breach	A personal data breach means the accidental or unlawful destruction, loss, alteration, disclosure or access to personal data. Breaches are either accidental or deliberate.
Automated decision making/profiling	This is when machines/software make decisions based on rules generated by the machine/software, without human intervention, about someone. Typically, it is the significance of the decision that drives the caution and concern here.

5.0 The data controller

Our school collects and processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. The school's registration number is **Z4758166**.

6.0 Data protection principles

The data protection principles require that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay, (taking into account the purpose for which it is being processed);
- Kept in a form that allows identification of data subjects for no longer than is necessary for the purposes for which it is processed;
- 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.

7.0 Processing personal data

7.1 Lawfulness

We will only process personal data where we have grounds for that processing to take place. This is called a 'lawful basis' (legal reason) for processing and there are six options depending on our purpose and relationship with the individual. No single basis is 'better' or more important that the others and are highlighted below:

- **Consent:** the individual (or their parent/carer when appropriate – see section 9.2) has given clear consent for the school to process their personal data for a specific purpose. Consent will be sought for some specific sensitive data e.g. biometric fingerprint and photographs. If we ask for consent to use personal information that consent can be removed at any time. Any use of information before consent is withdrawn remains valid. If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).
- **Contract:** the data needs to be processed so that the school can fulfil a contract we have with the individual, or the individual has asked the school to take specific steps before entering into a contract
- **Legal obligation:** the data needs to be processed so that the school can comply with the law (not including contractual obligations).
- **Vital interests:** the data needs to be processed to protect someone's life.
- **Public task:** the data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions. The task or function has to have a clear basis in law.
- **Legitimate interests:** the data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

For PHSG students the lawful bases will generally be 'legal obligation' and 'public task'. For PHSG staff the lawful basis will generally be 'necessary for a contract'.

7.2 Fairness and transparency

We will be clear, open and honest about the reasons we are collecting personal data and how we intend to use this. We will only process personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will produce Privacy Notices to inform individuals about the personal data we process, the reasons for this and who we may share this with. This will also inform them of their rights under the GDPR and DPA 2018. The Privacy Notices will be available via the school website and will be issued to new staff and students upon their initial admission to the school through the relevant induction booklet.

7.3 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. The information we collect will be relevant and limited to what is necessary to fulfil the purpose for which it is being collected. We will be clear from the outset the reasons why we are collecting personal data and what we intend to do with it. This applies whether we collect the personal data directly from the individual or whether we collect their data from another source.

If we want to use personal data for reasons other than those specified when we first collected it, we will ensure that the new use is fair, lawful and transparent. We will inform the individuals concerned before we do so, and seek consent where necessary.

We will take all reasonable steps to ensure that the personal data we hold is not incorrect or misleading and will keep this updated if this is necessary for the purpose we are using it. If we discover that personal data is incorrect or misleading we will take reasonable steps to correct or erase it as soon as possible.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

We will record our purposes for processing personal data in our data asset register and specify them in our privacy notice.

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- We need to liaise with other agencies – we will seek consent as necessary before doing this;
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;

- The assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy our safeguarding obligations;
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided;

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9.0 SUBJECT DATA RIGHTS OF INDIVIDUALS

9.1 Data protection rights of the individual

Individuals have certain rights under the DPA 2018 and the GDPR. These are detailed in the school's privacy notices. Individuals should contact the school's data protection officer if they would like to exercise any of their rights. If the school receives a request directly then they should contact the Data Protection Officer immediately. Please refer to the school's 'subject rights request policy' for full details of the access rights of the individual, how a request can be made and how we will respond to this.

9.2 Data protection rights of children

A child, (anyone under the age of 18) has the same data protection rights over their personal data as an adult. We will give personal data processed about our pupils' specific consideration as they may be less aware of the risks, consequences and safeguards concerned.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of processing their personal data. Therefore, the rights of most of our children, including consent, can be exercised by our pupils. Any request from parents or carers of our pupils may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis. If we judge a child is not mature enough to understand their rights, their rights, including consent, can be exercised by parents or carers without the express permission of the pupil, provided we are satisfied that the request has come from a person with parental responsibility.

10. REQUESTS TO SEE THE EDUCATIONAL RECORD (maintained school)

Pupils, (or parents/carers of a child who cannot act for themselves or who has given consent), have a legal right to free access to their/child's educational record (which includes most information about a pupil). Please see the school's SAR policy to see how we will assess if a child has capacity to make such a request. The information included in the educational record will cover academic achievements, correspondence from teachers, local education authority, employees, educational psychologists etc. It must be provided within one month of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's code of practice and their guidance for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr Shaun Willis, Headteacher

12. PHOTOGRAPHS AND VIDEOS

As part of our school activities, we may take photographs and record video images of individuals within our school.

We will obtain written consent from staff, parents/carers, or pupils (in line with section 9.2 of this policy – rights of children) for photographs and videos to be taken for communication, marketing and promotional materials. Any request for consent will clearly explain to staff, parent/carers or pupils what the photograph and/or video will be used for.

Consent can be refused or given for some or all of the purposes for which it is taken, for example:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can also be withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we may, with consent, include the child's first name, however we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Care will be taken to safeguard the device used to take photographs or video footage. Where possible the device will be encrypted and/or password protected and images/footage will be uploaded to the school's secure drive as soon as possible and then immediately deleted from the portable device. Images will not be stored to individual drives or to individual computer hard drives. Portable devices containing images not yet uploaded will be locked away when not in use.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

13. DATA PROTECTION BY DESIGN AND DEFAULT

The GDPR has placed a legal requirement on us to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual's rights. We have practises in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointment of a suitably qualified Data Protection Officer;
- Data protection issues are considered as part of the design and implementation of systems, services and business practices;
- We will notify the DPO where the school's processing of personal data presents a high risk to the rights of individuals, and when introducing new technologies in order to complete a data protection impact assessments (DPIA);
- Data protection issues are considered for any activities by the school, both on and off site. We will anticipate the risks to data privacy and take steps to prevent loss;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;
- Only using IT systems, services and business practices where personal data is automatically protected. We will ensure that the same standards of data protection are applied;
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Training members of staff at induction and at regular intervals on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- Making records of our processing activities available to individuals so that they can determine how we are using their personal data. This includes:
    - The name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For <u>all</u> personal data that we hold, maintaining an internal record (data asset register) of the type of data, how and why we are processing the data (including the lawful basis), how we control access and keep the data secure and retention periods.

14. DATA SECURITY AND STORAGE OF RECORDS

We will process personal data securely and protect it from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Our measures to achieve this include:

- Keeping paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data under lock and key when not in use;

- Not leaving papers containing confidential personal data on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- Where personal information is taken off site, staff must take care to treat this information with care and keep it secure at all times, e.g. not leaving personal data in the boot of a car or on display where others may gain access to it;
- Security software is installed on those computers containing personal data. Only authorised users are allowed access to the computer files. Computer files are backed up (i.e. security copies are taken) regularly.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals;
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, pupils or governors should not store personal data on their own personal devices.
- In exceptional circumstances and only where permission has been granted, if staff or governors do store personal data on their personal devices they are expected to follow the same security procedures as for school-owned equipment - see our acceptable use agreement;
- Where we need to share personal data with a third party, we carry out due diligence, put in place a data sharing agreement and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).
- We will not keep data for longer than we need it. Data will be retained in line with the Information and Records Management Society's toolkit for schools
- We will periodically review the data that we hold and securely dispose of or anonymise it when it is no longer needed.
- Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
- We will shred or incinerate paper-based records, and overwrite or delete electronic files. Hard drives will be wiped before physical destruction when they have reached the end of their life. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.
- Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in computer rooms. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

- In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All members of staff are trained in their Data Protection obligations and their knowledge updated as necessary.

15. PERSONAL DATA BREACHES

The school will take all reasonable precautions to ensure that there are no personal data breaches.

GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO). Where feasible this must 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 a 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.

Please refer to the school's 'Data Breach Management Policy' to see how we identify and manage personal data breaches.

16. MONITORING ARRANGEMENTS

This policy will be reviewed and updated if necessary **every 2 years**, or sooner if a security loophole or data breach is identified, and shared with the full governing board.