PLYMOUTH HIGH SCHOOL FOR GIRLS

POLICY: **DATA PROTECTION POLICY**

SLT LINK MEMBER:	**Mary Utton**
GOVERNORS SUB COMMITTEE:	**P & R**
This policy was adopted/updated:	January 2014
This policy will be reviewed:	January 2016
Statutory Policy:	NO
Source:	School

Plymouth High School for Girls

Data Protection Policy

Plymouth High School for Girls collects and uses personal information about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The School is registered with the Information Commissioner's Office as data controller detailing the information held and its uses and will ensure that processing of personal data is carried out in accordance with its registration and the principles of the Act. The School also has a duty to issue a Fair Processing / Privacy Notice to all students/parents. This summarises the information held on students, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. This policy applies to all staff and governors. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information which is in the possession of, or is likely to come into the possession of, the data controller.

Data is information which is recorded or processed either automatically by the use of equipment (i.e. computer) or as part of a relevant filing system or record defined in the Act.

A relevant filing system is a system is a system structured in such a way that specific information relating to a particular individual is readily accessible.

The Act identifies some data which is to be given a higher level of protection. This is called Sensitive Personal data and is personal data about the subject's:-

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence – this includes any proceedings for any offence committed or alleged to have been committed by the data subject, the outcome of those proceedings, including the sentence of any court

The School will ensure that Sensitive Personal data receives the highest level of protection under the Act as required with the First Principle.

Processing personal data describes the action taken with the data, including obtaining, recording, holding, storing and destroying the data.

Registered Purposes

Mr Paul Renyard, Business Manager, is the nominated person dealing with data protection issues and acts as the contact point regarding the School's Data Protection Act Registration entries and for any subject access requests. Registered purposes covering the data held at the school are listed on the school's registration and data collection documents. Information held for these stated purposes will not be used for any other purposes without the data subject's consent.

Data Protection Principles

This Policy sets out the School's commitment to upholding the Data Protection principles set out in the Act. The Act establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Statement

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

- Inform individuals, where it acts as Data Controller, the reasons for data collection, the purposes for which data is held, the likely recipients of the data and the data subjects' right of access.
- Print on the appropriate collection form information about the use of personal data. If details are given verbally, the person collecting the data will explain the issues before collection of information.
- Inform individuals when their information is shared, and why and with whom.
- Hold the minimum personal data necessary to carry out its functions, ensuring data will be adequate, relevant and not excessive in relation to the purpose for which the data is held. In order to ensure compliance with this, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact the subjects to verify certain items of data. Records are checked for irrelevant data every twelve months and the decisions about what can be deleted is made by Mr P. Renyard.
- Check the quality and the accuracy of the information it holds and that it is as up-to-date as is reasonably possible.
- Update the computer record as soon as is practicable if a data subject informs the School of a change of circumstances.
- Provide to any data subjects every twelve months a printout of their data record so they can check its accuracy and make any amendments.
- Immediately mark the record as potentially inaccurate where a subject challenges the accuracy of their data. Until resolved, the information will be marked and both versions will be saved.
- Ensure that information is not retained for longer than is necessary for the purposes registered.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely provided the retention periods required by law have been met. It is the duty of Mr P. Renyard to ensure that obsolete data are properly erased.

- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as subject access requests (SARs)
- Ensure our staff are aware of and understand our policies and procedures and provide training designed to ensure the principles are upheld throughout the organisation.

Rights of the Individual
The individual is entitled:-

a. To ask the authority if it holds information about them.
b. To ask what it uses the information for.
c. To be given a copy of the information (excluding any information exempt from disclosure under the Act.
d. To be given details about the purposes for which the authority uses the information and of other organisations or persons to whom it is disclosed.
e. To ask for incorrect data to be corrected.

Information to Parents / Carers – the "Privacy Notice" (formerly referred to as "Fair Processing Notice")
Under the "Fair Processing / Privacy" requirements in the Data Protection Act, the school will inform parents / carers of all students of the data they hold on the students, the purposes for which the data is held and the third parties (eg LA, DfE, QCA, Careers South West etc) to whom it may be passed. This Privacy Notice will be passed to parents / carers through the school website. Parents / carers of young people who are new to the school will be notified where they can access the Privacy Notice through the Prospectus and Induction Booklet.

See **Appendix 1** for procedures on **subject access requests (SARs)**.

Data and Computer Security
The School undertakes to ensure security of personal data by the following general methods (precise details cannot be revealed):

1. **Physical Security**
   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.

2. **Logical Security**
   Security software is installed on those computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

3. **Procedural Security**
   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. Computer printouts as well as source documents are shredded or incinerated before disposal.

Overall security policy for data is determined by the Headteacher and the Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The School's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the school should in the first instance be referred

to Mr P. Renyard.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

For further procedure on Data Protection with regard to data held electronically refer to the School's **E-Safety Policy**.

Complaints
In cases of dispute, the School will attempt to resolve the issue informally, but if this proves impossible, disputes will be dealt with in accordance with the school's complaints policy. If the dispute cannot be resolved at this stage, either side may seek independent arbitration and complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745 3

Appendix 1

Plymouth High School for Girls
Procedures for responding to subject access requests (SARs) made under the Data Protection Act 1998

Rights of access to information
There are two distinct rights of access to information held by schools about students.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to **Paul Renyard, Business Manager.** If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
   - passport
   - driving licence (photo card not paper copy)
   - utility bills with the current address
   - Birth / Marriage certificate
   - P45/P60
   - Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The School will keep a log of requests that require formal consideration showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date).

5. The school may make a charge for the provision of information, dependent upon the following:
   - Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
   - Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
   - If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

6. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**.

However the 40 days will not commence until after receipt of fees or clarification of information sought.

7. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

8. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

9. **Authorised Disclosures**
   The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which Plymouth High School for Girls authorised officer may need to disclose data without explicit consent for that occasion.
   These circumstances are strictly limited to:
   - Student data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
   - Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.
   - Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within the vicinity of the school.
   - Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
   - Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school.
   - Only authorised and trained members of staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work.

10. Any information which may cause serious harm to the physical or mental health or emotional condition of the student or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

11. If there are concerns over the disclosure of information then additional advice should be sought.

12. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

13. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

14. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints
Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.
Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts
If you have any queries or concerns regarding these policies / procedures then please contact **Mr Paul Renyard, Business Manager**.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone