THE PERSE SCHOOL
CAMBRIDGE

Data Protection Policy

1. Introduction

This policy explains the Data Protection Principles and sets out the School's obligations under the Data Protection Act 1998 (the "Act"). The purpose of the Act is to safeguard personal information and it covers issues such as data security, individuals' rights to access information about them and the use and disclosure of personal data.

Background: This policy is aimed at all staff at the School including temporary staff, agency workers and volunteers. It also applies to Governors. It explains the School's approach to data protection and provides practical guidance which will help to ensure that the School complies with the Data Protection Act.

Responsibility: Compliance with this policy will help the School to meet its obligations under the Act but this policy does not commit the School to a higher standard than is required by the Act. In some circumstances, e.g. situations involving safeguarding concerns, strict compliance with the Act will be subsidiary to other considerations.

Relevance: Data protection is important because it concerns an individual's right that their personal information is used in a manner that is fair and lawful. A breach of the Act could have serious consequences for the individual, the School and its staff. **A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.**

Data Protection Controller (DPC): The Governors have appointed the Bursar as the School's Data Protection Controller who will endeavour to ensure that all personal data is processed in compliance with this policy.

An important part of this policy is **section 9** below which concerns information security. It sets out the steps which staff must take to help ensure that Personal Data is not lost, misplaced or accidently disclosed to third parties. **Please make sure that you have read and understood this section in particular.**

This policy is intended to give an overview of the Act and staff obligations. This policy should be read alongside the following:

Acceptable Use of ICT - Staff;
Privacy notices for pupils and parents – How we use your information
Records Management Guidance; and
Managing Images of Children Policy

2. Definitions and scope of the Act

Personal Data: "Personal Data" means any information relating to an identified or identifiable natural person. "Identifiable" means one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity. This means that a document might contain Personal Data about someone even if they are not named, (eg, if it was obvious who was being referred to).

Sensitive Personal Data: "Sensitive Personal Data" includes information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical/mental health or condition, sexual life, actual or alleged criminal offences and sentences imposed.

Sensitive Personal Data will generally be processed only where one of the following conditions applies:

- The Data Subject has/have given explicit consent;
- The processing is necessary to protect vital interests; or
- There is a medical or statutory requirement to process the data

Processing: "Processing" may include creating, obtaining, recording, holding, disclosing, amending, destroying or otherwise using personal data. This means that the School will be caught by the Act just by storing Personal Data. The School may process a wide range of Personal Data of pupils, their parents or legal guardians, staff, volunteers and Governors as part of its operation.

Exemptions: Certain data are partially exempt from the provisions of the Act. Such data includes Personal Data processed in connection with the prevention or detection of crime and Personal Data processed in connection with business planning.

The above are examples and are only partial exemptions. Any further information on exemptions should be sought from the DPC.

The Act applies to Personal Data held on computer. This is the case regardless of how the information is held. For example Personal Data stored in an email, in a spreadsheet or on a smartphone, are all caught by the Act. Recorded CCTV images and sound recordings might also contain Personal Data.

The Act also applies to most paper records. Although some paper records are not covered by the Act, there are so many exceptions that best practice is to treat all paper records as being covered and therefore be subject to the Act. For example, some health records prepared by a doctor, nurse or other health professional are covered by the Act no matter how they are held.

Virtually any information about someone is likely to be Personal Data. All of the following examples are likely to contain Personal Data and are therefore subject to the Act:

- Information about a child protection incident;
- A record about disciplinary action taken against or an investigation into a member of staff;
- Photographs of pupils;
- A tape recording of an interview or meeting;
- Contact details and other personal information held about pupils, parents and staff and their families;
- Contact details of a member of the public who is enquiring about placing their child at a School;
- Financial records of a parent; and
- Records of staff sickness absence or compassionate leave.

3. The Data Protection Principles

In accordance with the eight Data Protection Principles in the Act, the School must ensure that all Personal Data is:

- Fairly and lawfully processed;
- Processed for a specified lawful purpose;
- Adequate, relevant and not excessive;
- Accurate and kept up-to-date;
- Not kept for longer than necessary;
- Processed in accordance with the Data Subject's rights;
- Secure; and
- Not transferred to other countries without adequate protection

What these obligations mean in practice is explained below.

4. Data protection in practice

Purposes of Processing Personal Data

Personal Data should only be used for specific and legitimate purposes. In the case of the School these are:

- Providing pupils and staff with a safe and secure environment, an education and pastoral care;
- Providing activities for pupils and parents - this includes school trips and activity clubs;
- Providing academic and examination references for pupils;
- Providing employment references for pupils and staff;
- Administering the recruitment and employment of staff;
- Safeguarding and promoting the welfare of children;
- Protecting and promoting the interests and objectives of the School - this includes fundraising; and
- Fulfilling the School's contractual and other legal obligations.

School staff must not Process Personal Data for any other purpose without the DPC's permission.

Staff should not use Personal Data for any purpose that is incompatible with the purpose for which it was originally acquired without obtaining the DPC's permission.

5. Disclosing Personal Data

Staff will frequently disclose Personal Data for legitimate professional purposes. For example staff may routinely discuss a pupil's academic progress with parents.

This is allowed by the Act, but staff should not disclose Personal Data in circumstances which might be considered unusual, or where the Personal Data includes Sensitive Personal Data, without permission from the DPC. Staff should always speak to the DPC if in doubt about whether a disclosure of Personal Data is permissible.

Staff must not transfer Personal Data outside the European Economic Area (EEA) without obtaining the DPC's permission.

6. Handling Personal Data in general

- Staff must not use Personal Data for any purpose that is incompatible with the purpose for which it was originally acquired without obtaining the individual's permission. Staff should seek advice from the DPC in all but the clearest of cases, but if information has been obtained in confidence for one purpose, it must not be used for any other purpose without authorisation from the DPC.
- The School must Process Personal Data in a way that is fair to individuals. Following this policy is likely to mean that the Processing is fair in most cases. However, the concept of fairness can be quite difficult to define and staff should inform the DPC if they feel that any of the Processing of Personal Data appears to be unfair to any individual in any way even if the Processing appears to comply with this policy.
- The School must only keep Personal Data for as long as is reasonably necessary but staff should not delete records containing Personal Data without authorisation. Staff should consult the School's Records Management Guidance for guidance on data retention.
- Staff should ensure that Personal Data is complete and kept up-to-date. For example, if a parent notifies a member of staff that their contact details have changed, the member of staff should inform the School Office so that the School's central record can be updated.
- The School must ensure that it has sufficient Personal Data. For example a teacher writing a report about a pupil should ensure that he/she has all the pupil's relevant records including learning support information to hand.
- The School must not process Personal Data in a way that is excessive or unnecessary. For example:
    - Where 8 pupils out of a class of 20 attend a field trip, the member of staff should only take records (such as information about allergies and parent contact details) of those 8.
    - Personal Data held on individual staff personnel files must relate only to that individual. Eg payroll instructions must be specific to the individual concerned, or on separate sheets for filing. This is to ensure that Personal Data of staff is not disclosed inadvertently.

7. Informing the individual

- Individuals must be told what data is collected, and what it is used for, unless it is obvious. This is sometimes called a privacy notice or fair processing statement Individuals should also be told which third parties (if any) it will be shared with and anything else which might be relevant.
- Staff are not expected to routinely provide pupils, parents and others with a privacy notice as this should have already been provided. Copies of the parent and pupils privacy notices can be found on the school's website.

  Having said this, staff should inform the DPC if they suspect that the School is using Personal Data in a way which might not be covered by an existing fair processing notice. This may be the case where, for example, staff are aware that the School is collecting medical information about children without telling their parents what that information will be used for.

8. Sharing Personal Data

The general position is that Personal Data should only be shared on a "need to know" basis. Before sharing Personal Data staff should:

- Make sure they are allowed to share it;
- Ensure adequate security (please see section 9 below); and
- Make sure that the sharing is covered in the School's privacy notices for pupils and parents (please see section 7).

Sharing Personal Data within the School

- This section applies when Personal Data is shared within the School.
- Personal Data must only be shared within the School on a "need to know" basis although this will not prevent sharing Personal Data where doing so is reasonable and proportionate and is done in accordance with this policy.
- Staff should think about whether the person(s) they wish to share the Personal Data with needs access to the information
- Examples of sharing which are likely to comply with the Act:
  - A teacher discussing a child's academic progress with other members of staff (for example, for advice on how best to support the child);
  - Informing an exam invigilator that a particular pupil suffers from panic attacks;
  - Disclosing details of an assistant's allergy to bee stings to colleagues so that they will know how to respond. Other private health matters must still be kept confidential and advice should be sought from HR or the Assistant Bursar if in doubt).
- Examples of sharing which are unlikely to comply with the Act:
  - The Head being given access to all records kept by nurses working within the School (seniority does not necessarily mean a right of access);
  - Informing all staff that a pupil has been diagnosed with dyslexia (rather than just those who teach the pupil);
  - Disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or unless it is an emergency).

Sharing Personal Data with individuals and organisations outside of the School (for example, with other schools, colleges, social services, the Police, and contractors)

- Sharing Personal Data with others is often permissible so long as doing so is fair and lawful under the Act but staff should always speak to the DPC if in doubt, or if staff are being asked to share Personal Data in a new way.
- Before sharing Personal Data outside of the School staff should:
  - Make sure that they are allowed to share it;
  - Ensure adequate security (please see section 9 below). What is adequate will depend on the nature of the data. For example, if the School is sending a child protection report to social services on a memory stick then the memory stick must be encrypted; and
  - Make sure that the sharing is covered in the privacy notices for pupils and parents (please see section 7).
- The School should ensure that any emails which contain Sensitive Personal Data are encrypted. This includes emails sent to parents.
- Staff should not disclose Personal Data to the Police without permission from the DPC (unless it is an emergency). The Police are required to request Personal Data formally using an appropriately worded form.
- Staff must not disclose Personal Data to contractors without permission from the DPC. This includes, for example, sharing Personal Data with an IT contractor (e.g., where the contractor is to carry out a data cleansing exercise).
- Permission should be sought from the DPC before publishing anything containing Personal Data (for example, uploading photographs of a trip organised by the School to one of the School's websites).
- Staff should be aware of the use of deceit to obtain personal data from people or organisations. Staff should seek advice from the DPC where staff are suspicious as to why the information is being requested or if they are unsure of the identity of the requester (e.g. if a request has come from a parent using a different email address).

9. Protecting Personal Data and Information Security

- **Information security is the most important aspect of data protection compliance**. Most of the fines under the Act relate to security breaches such as leaving an unencrypted memory stick in a public place, sending sensitive documents to the wrong recipient, disposing of confidential documents without shredding them first or accidentally uploading confidential information to the web. Staff must do all that they can to ensure that Personal Data is not lost or damaged, or accessed or used without proper authority.
- The Act requires the School to take organisational measures (for example, ensuring that staff are trained on information security), and technical measures (for example, encryption, secure shredding etc) to ensure that Personal Data is kept secure. These requirements are explained in more detail below and should be read in conjunction with the School's Acceptable Use of ICT - Staff and Records Management Guidance.

- Staff must:
    - Ensure that their use of Personal Data is necessary and proportionate. For example, staff must not take Personal Data off School premises unless there is a genuine need (subject to the other provisions of this policy).
    - Immediately report all security incidents, breaches and weaknesses, to the DPC. This includes anything which the member of staff becomes aware of even if they are not directly involved (for example, if a teacher notices that document storage rooms are sometimes left unlocked at weekends).
    - Be very careful when sending correspondence containing Personal Data (e.g., sending a fax, an email, or sending documents by post). Staff should check that they are sending the correct Personal Data to the intended recipient very carefully and ideally should ask an appropriate colleague to check both the data to be sent and the individual recipient for accuracy. Extreme care must be used with attaching files to emails.
    - Comply with any School procedure relating to the handling of Personal Data (e.g., booking out and booking in School laptops);
    - not use or leave computers, portable electronic devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: staff should take reasonable steps to ensure that such devices are not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.
    - Be vigilant of the risks posed by cameras on mobile phones. As such, Sensitive Personal Data should always be carried in sealed envelopes / folders to avoid it being photographed.
- The School uses a range of measures to protect Personal Data stored on computers, including, anti-virus and security software, user passwords, and back-up systems. These should be used in all cases.
- Staff must not remove Personal Data from the Schools' premises. Staff should use the remote desktop facility to access Personal Data. If a member of staff needs to take Personal Data off-site, they need to consult with the DPC.

Personal Data held on computer

- With regards to the security of Personal Data held on computer staff must:
    - Not download Personal Data relating to the School to their own computers or send such Data to their own email accounts. For example, they must not send School related emails containing Personal Data to their private email account.
    - Not use their own devices to store or transport School Personal Data and must instead only use devices issued by the School (and in any even permission should be obtained before taking Personal Data off School site - please see above).
    - Not allow unauthorised access to School computers or other computers containing School related Personal Data. For example, staff should not allow pupils or their friends and family access to their work computers or work emails.
    - Use bcc (blind carbon copy) where appropriate;
    - Lock their computers when not in use;
    - Keep any passwords secure although passwords are not always effective and are not a substitute for encryption. Passwords should contain at least eight characters, use special symbols, be difficult to guess, and should be changed frequently.

- Encryption should be used, when handling personal, sensitive or confidential data. This includes saving internally on the school systems and when transferring data to external entities (please refer to the document *How to Encrypt* which can be found within the IT Guidance on SharePoint).

Personal Data held in hard copy / paper form

- With regards to the security of Personal Data held in physical form (e.g. paper files) staff must:
    - Ensure that any such records are kept under lock and key in a secure location;
    - Be very careful if sending the Personal Data by fax. Not only should staff ensure that the correct fax number is used but staff should ensure that the recipient is waiting to collect the fax at the other end;
    - Take extra precautions in relation to any Sensitive Personal Data and any Personal Data which is particularly confidential, both of which should be stored in a storage room or in a strong cabinet (again under lock and key); and
    - Ensure that documents containing Personal Data are never be left unattended on desks (unless the room is secure).
- Staff must comply with the School's Acceptable Use of ICT - Staff. In particular staff must not:
    - do anything to compromise the security of any of the School's systems;
    - change any privacy settings or connect any device that has not been provided by the School (such as a memory stick);
    - click any links in documents or emails, unless the member of staff is absolutely sure that source is trusted; or
    - attempt to gain unauthorized access to any part of the School's ICT system.
- Staff acknowledge and agree that the School may monitor and access any part of the School ICT system for any purpose connected with the operation of the School. The School ICT system includes any hardware, software, email account, computer, device, or telephone, provided by the School. The purposes of such monitoring and accessing include:
    - To help the School with its day to day operations. For example if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and
    - to check staff compliance with this policy, and the School's other policies and procedures. For example to investigate allegations that a member of staff has been using their email account to send abusive messages.
- Some School Personal Data is so sensitive that it must never be taken off site, and / or accessed by staff using their own devices, without specific permission from the Bursar. This includes:
    - Information concerning child protection matters;
    - Information about serious or confidential medical conditions and information about special educational needs;
    - Information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);

- Financial information (eg, about parents and staff); and
- Any other information which falls within the definition of Sensitive Personal Data under the Act. This is information about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life and information relating to actual or alleged criminal activity.

10. Disposing of Personal Data

- Any record containing Personal Data should be securely destroyed, in accordance with the appropriate retention period as indicated in the Records Management Guidance;
- Personal Data must not be kept for longer than is necessary;
- any paper documents should be shredded or placed in the confidential waste bins provided and CDs, memory sticks and other storage media should be physically destroyed when they are no longer required;
- when disposing of computer records containing Personal Data it is important to make sure that the record is permanently deleted. It is not sufficient just to move the file into the recycle bin. Specialist software should be used to permanently delete the computer record. Further information is available from the DPC; and
- paper records should be disposed of securely using the School's procedures. For example, if a member of staff is working from home then they should return any paper waste to the School to be securely disposed of.

11. Data Protection related Requests from Individuals

Individuals have a number of rights under the Act. One of the most commonly exercised is the right to request a copy of the Personal Data the School holds about them. This is called a Subject Access Request.

- Any staff who receive a Subject Access Request must promptly forward it to the DPC, which should in most cases be the same day. This is important as there is a statutory procedure and timetable which the School must follow. Staff must never respond to a Subject Access Request themselves unless authorised to do so.
- Staff should be aware that there is no obligation to refer to the "Data Protection Act" or the phrase "Subject Access Request" when making a request. By way of an example, an email which simply states "Please send me copies of all emails you hold about me" is a valid Subject Access Request.
- Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should a Subject Access Request be made. There is no exemption for "embarrassing" information. For example, an exchange of emails containing gossip about an individual will usually be disclosable. **As such staff must be aware that anything they put in an email is potentially disclosable.**

12. Other rights

- Individuals have a number of rights under the Act in addition to the right to make a Subject Access Request. This includes a right to:
  - Prevent the use of their data for marketing;
  - Ask to have inaccurate data amended;

- Prevent the use of data in a way that is likely to cause unwarranted substantial damage or unwarranted substantial distress to themselves or anyone else; or
- Object to any decision that significantly affects them being taken solely by a computer or other automated process. *For example, basing salary increases solely on a pre-determined formula without giving the employee an opportunity to object or make representations.*

- Any members of staff who receive a request which relates to any of the above must promptly forward it to the DPC.

13. Further information

- If staff have any questions about this policy or about data protection they should speak to the DPC.
- Similarly, all staff have an obligation to assist the School and colleagues to comply with the Act. Therefore staff should also report any concerns, or any evidence of non-compliance, to the DPC.
- We have registered our use of Personal Data with the Information Commissioner's Office and further details of the Personal Data we hold, and how it is used, can be found in our register entry on the Information Commissioner's website at www.ico.gov.uk under registration number **Z1019296**. This website also contains further information about data protection.

Authorised by:	Sir David Wright On behalf of the Board of Governors
Date	28th June 2016
Review Date	June 2017