Foremarke Hall
Repton Preparatory School

Policy Statement

Data Protection Policy

DATA PROTECTION POLICY

Introduction

1. **Application:** This Policy is aimed at all School staff including temporary staff, agency workers and volunteers. It also applies to Governors and contractors. It explains the School's general approach to data protection, and provides practical guidance which will help to ensure that the School complies with the Data Protection Act 1998 (the Act).

2. **Compliance:** Compliance with this policy will help the School to meet its obligations under the Act but it does not commit the School to a higher standard than is required by the Act and in some circumstances, where the Act allows, compliance with the Act will be subsidiary to other considerations.

3. **Responsibility:** As the Data Controller, the School is responsible for complying with the Act. The Governing Body has delegated day to day responsibility for compliance with the Act to the Bursar. All staff are responsible for complying with this policy.

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

   4.1 IT Acceptable Use Policy; and

   4.2 Fair Processing Statement.

   This list is not exhaustive.

5. 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 fax recipient, disposing of confidential documents without shredding them first or accidentally uploading confidential information to the web. Further information can be found below under paragraph 25.

Terminology

6. **Terminology:** In this policy, the School has used the terms Personal Data, Sensitive Personal Data, Data Controller and processing in the same way as they are used in the Act.

7. **Personal Data:** This policy covers the School's acquisition and use of the Personal Data it holds, and in particular records about pupils, parents, staff and suppliers. Personal Data is:

7.1 personal information that has been, or will be, word processed or stored electronically (e.g. computer databases and CCTV recordings);

7.2 personal information that is, or will be, kept in a file which relates to an individual or in a filing system that is organised by reference to criteria which relate to the individuals concerned (e.g. name, school year, school activities); and

7.3 health records prepared by a doctor, nurse or other health professional.

8. Personal information is any information about someone who can be identified (e.g. their address, school activities, attendance record, exam results). It makes no difference whether they can be identified directly from the record itself or indirectly using other information.

9. The Data Subject is the person the information relates to. There may be more than one Data Subject, such as when a record concerns an incident involving two pupils.

10. **Sensitive Personal Data**: The School has special obligations in connection with the use of Sensitive Personal Data, namely information about an individual's race, ethnic origin, political or religious beliefs, trade union membership, health, sex life and actual or alleged criminal activity.

11. **Data Controller:** For the purposes of the Act, the School is the Data Controller.

Acquiring and using Personal Data

12. **Specific legitimate purposes:** The School shall only process Personal Data for specific and legitimate purposes. These are:

12.1 ensuring that the School provides a safe and secure environment;

12.2 providing pastoral care;

12.3 providing education and learning for children;

12.4 providing additional activities for children and parents (for example activity clubs) ;

12.5 protecting and promoting the School's interests and objectives - this includes fundraising;

12.6 safeguarding and promoting the welfare of children;

12.7 for personnel, administrative and management purposes - for example: to pay staff and to monitor their performance;

12.8 to fulfil the School's contractual and other legal obligations.

13. School staff must not process Personal Data for any other purpose without the

Bursar's permission.

14. **No incompatible purpose:** The School shall not use Personal Data for any purpose that is incompatible with the purpose for which it was originally acquired without obtaining the Data Subject's permission. Staff should seek advice from the Bursar in all but the clearest of cases, but if information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the Bursar's permission.

15. **Necessary, sufficient information:** The School shall not hold unnecessary Personal Data, but shall hold sufficient information for the purpose for which it is required. The School shall record that information accurately and shall take reasonable steps to keep it up to date. This includes an individual's contact and medical details.

16. **Outside the EEA:** The School shall not transfer Personal Data outside the European Economic Area (EEA) without the Data Subject's permission unless it is satisfied that the Data Subject's rights under the Act will be adequately protected and the transfer has been approved by the Bursar. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

17. **Fair:** When the School acquires personal information that will be kept as Personal Data, the School shall be fair to the Data Subject and fair to whoever provides the information (if that is someone else).

18. **Retaining Personal Data:** The School shall only keep Personal Data for as long as is reasonably necessary. More specific guidelines apply in particular situations: further details are available from the Bursar.

Information and explanation

19. **Explanations when asking for Personal Data:** Unless it is already clear to the person concerned, when the School asks for personal information which may be kept as Personal Data the School shall:

    19.1 explain which information is optional, which is mandatory, and the consequences if it is withheld;

    19.2 explain why the School is asking for that information, and how it will be used;

    19.3 identify the School as the Data Controller; and

    19.4 explain who outside the School will receive that information.

20. **Informing the Data Subject:** If the School obtains personal information from someone other than the Data Subject, the School shall:

    20.1 inform the Data Subject that the School has recorded that information;

    20.2 identify its source;

    20.3 explain why the School has acquired it, and how it will be used;

    20.4 identify the School as the Data Controller; and

20.5 explain who outside the School will receive that information.

21. A different approach may be necessary when medical, child protection or staff issues are involved; further advice is available from the Bursar.

Protecting confidentiality

22. **Disclosing Personal Data within the School:** Personal Data should only be shared on a need to know basis. Personal Data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the School or their relationship to the Data Subject, unless they need to know it for a legitimate purpose. Examples include:

    22.1 the School Nurse may disclose details of a lunchtime supervisor's allergy to bee stings to colleagues so that they will know how to respond, but more private health matters must be kept confidential;

    22.2 personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and email address) shall not be disclosed to parents, pupils or other members of staff unless the member of staff has given their permission.

23. **Disclosing Personal Data outside of the School:** Sharing Personal Data with others is often permissible so long as doing so is fair and lawful under the Act. However, staff should always speak to the Bursar if in doubt, or if staff are being asked to share Personal Data in a new way.

24. The School should be careful when using photographs, videos or other media as this is caught by the Act as well.

25. Information security and protecting Personal Data: Most of the fines under the Act relate to security breaches. The School shall do all that it can to ensure that Personal Data is not lost or damaged, or accessed or used without proper authority, and the School shall take appropriate steps to prevent these events happening. In particular:

    25.1 paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended. The records should be kept in a secure location;

    25.2 the School uses a range of measures to protect Personal Data stored on computers, including file encryption, anti-virus and security software, user passwords, audit trails and backup systems;

    25.3 staff must keep any passwords secure although passwords are not always effective and are not a substitute for encryption. Further information is available from the IT Manager;

    25.4 staff must not remove Personal Data from the School's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the IT Manager;

25.5 cloud storage: information should not be stored in the "cloud" unless it is encrypted first[1];

25.6 staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased;

25.7 staff should be very careful when sending correspondence containing Personal Data (for example, fax numbers and email addresses should be double checked);

25.8 Personal Data must not be kept for longer than is necessary and any record containing Personal Data should be securely destroyed.

Staff must not handle confidential or Sensitive Personal Data when working from home, without prior authorisation.

Requests for information by Data Subjects

26. **Data Subject access request:** Individuals are entitled to know whether the School is holding any Personal Data which relates to them, what that information is, the source of the information, how the School uses it, and who it has been disclosed to.

27. **Use of personal data:** Individuals have a legal right to ask the School not to use their Personal Data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.

28. **Corrections:** Individuals have a legal right to ask for incorrect Personal Data to be corrected or annotated.

29. **Automatic decisions:** Individuals have a legal right to ask the School not to make automatic decisions (using Personal Data) if such automatic decisions would affect them to a significant degree.

30. **Receiving a request:** Any member of staff who receives a request for information covered by this policy from a pupil, parent or any other individual must inform the Bursar as soon as is reasonably possible, 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.

31. **Making a request:** Any member of staff wishing to exercise a right to request information covered by this policy, can do so by submitting a request in writing to the Bursar, and by paying the appropriate fee.

[1] Not all information needs to be encrypted first, for example this will not be necessary when dealing with low risk data. However, where sensitive confidential personal data is handled, encryption should be used.

Further information

32. **ICO website**: The School has registered its use of Personal Data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website at www.ico.org.uk under registration number Z5039885. This website also contains further information about data protection.

33. **Contact:** If you would like any further information about anything within this policy, please contact the Bursar.

Breach of this policy

34. 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.

Review Date
Last reviewed Lent 2016
Next review Lent 2017