St Peter's Church of England (VC) Primary School

Data Protection Policy

As a Rights Respecting School we recognise Article 16 'The right to privacy' from the UN Convention of the Rights of the Child.

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

St. Peter's School collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by St. Peter's School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

2. The Eight Principles

The Data Protection Act is based on eight data protection principles, or rules for good information handling.

1. Data must be obtained and processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

School staff should follow the KCC guidance on data protection when requesting, sharing or processing information.

Staff working at home or off the school premises, should follow the KCC Homeworking Data Protection Guidance, appendix 1.

Approved March 2017

Staff sharing information should always keep a written record of the reasons for request, thus complying with the HM Government "Seven golden rules for information sharing".

When making decisions in respect of the handling of personal information, the JAPAN Test should be used to decide if the need to share is Justified, Authorised, Proportional Auditable and Necessary.

Responsibilities

St. Peter's School must:

- Manage and process personal data properly
- Protect the individuals" right to privacy
- Provide an individual with access to all personal data held on them.

St. Peter's School has a legal responsibility to comply with the Act. St. Peter's School, as a corporate body, is named as the Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

St. Peter's School is required to notify the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link:
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

Every member of staff that holds personal information has to comply with the Act when managing that information.

St. Peter's School is committed to maintaining the eight principles at all times. This means that St. Peter's School will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice.
- check the quality and accuracy of the information held
- apply the records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act (see appendix e).
- train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures
- When sharing personal information outside the organisation and / or internal systems, 'best practice' protocols should always be followed:

If a request has been made of a school staff member to share information electronically:

- The electronic file should be password protected before sharing.
- An initial email should be sent to the recipient stating that a file containing personal information will follow. It should also contain the password for the file.

- A second email should be sent containing the file of personal information. It should also include a reminder for the safe, sensitive and confidential management of the personal information.
- It is always preferable to use a secure email address where available to contact / share information with other professionals.
- Initials of pupils and adults should be always be used in email correspondence when contacting other professionals to reduce to ensure the safety and security.

If a request has been made of a staff member to share information over the telephone

- St. Peter's School staff should ask for the name of the person making the request. The professional (land line) telephone number of the other professional should be taken and, where possible, phone contact should go through a switchboard. A return call will need to be made – to ascertain the identity of the person making the request.
- School staff should end the call at this point.
- The call should be returned immediately and once the other professional has been identified, within their organisation, the information should then be shared.

If a request has been made of a staff member to share information by post:

- St. Peter's School staff should share the information required, in a sealed envelope, using initials where appropriate.
- If an envelope with a clear window is used, the letter within should be folded in such a way as to hide the personal information.

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

Please follow this link to the ICOs website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact

Michelle Hunt
Access to Information Co-ordinator
Children, Families & Education
Tel: 01622 6969692
Email: michelle.hunt@kent.gov.uk

EQUALITY, SAFEGUARDING AND EQUAL OPPORTUNITIES STATEMENT

St Peter's School, in all policies and procedures, will promote equality of opportunity for students and staff from all social, cultural and economic backgrounds and ensure freedom from discrimination on the basis of membership of any group, including gender, sexual orientation, family circumstances, ethnic or national origin, disability (physical or mental), religious or political beliefs.

St Peter's School aims to:

- Provide equal opportunity for all
- To foster good relations, and create effective partnership with all sections of the community
- To take no action which discriminates unlawfully in service delivery, commissioning and employment
- To provide an environment free from fear and discrimination, where diversity, respect and dignity are valued.

All aspects of Safeguarding will be embedded into the life of St. Peter's School and be adhered to and be the responsibility of all staff.

Approved March 2017

APPENDIX 1

Homeworking - Data Protection Guidance

Introduction

The Data Protection Act 1998 is a law which governs the use of information that can identify individuals. This does not only apply to particularly sensitive information, and can be as little as name and address. The Act requires data controllers to have in place adequate security precautions to prevent unauthorised access, alteration or disclosure of personal information and to guard against its deliberate or accidental loss or destruction. The responsibility for individuals' data held by KCC extends to all work undertaken on behalf of the organisations by employees whether office based, mobile or home-based.

An increasing number of staff work at home either as part of their agreed working arrangements or on an ad-hoc basis according to work demands and individual preference.

This guidance has been produced to ensure those employees who work at home are aware of the security precautions required to protect the sensitive data they handle. All managers must ensure that staff for whom they are responsible who process personal data receive education and training in data protection issues and have up to date knowledge in this area.

Data Collection

Employees must ensure that to the best of their knowledge the personal data held on their equipment or in paper files is as accurate as possible, relevant, up to date and not kept longer than is necessary. Individual's from whom data is collected must be informed as to the purposes for which the data will be retained and used, including how it will be held and shared. They must be made aware of their rights to have access to their records and to comment on or correct inaccuracies. They must be informed of how to complain if they are unhappy with the way in which their information or their requests for access are handled.

Information that can identify individuals must be

- HELD - securely and confidentially
- OBTAINED - fairly and efficiently
- RECORDED - accurately and reliably
- USED - fairly and ethically
- SHARED - appropriately and lawfully.

All employees are responsible for reporting any breaches of security to their line manager.

Computerised Data

KCC Computers

Employees using KCC computers at home should ensure that normal security measures are followed to protect data and that up-to-date virus checking software is installed. PCs and laptops should be sited away from prying eyes and secured where possible. They should not be left where visitors to the house can easily access them. Back-ups of the data should be taken at regular intervals and not stored with the computer. If there are no back-ups and the equipment was to be stolen the information would be lost. When employees leave and their equipment is re-assigned elsewhere the information should be uploaded as necessary and deleted from the PC so as not to breach confidentiality.

Passwords
KCC computers are password protected to ensure that only those with authorisation can gain access to the system. To further minimise security risk passwords should not be shared with colleagues, other members of the household or anyone else and should also be changed frequently to protect the system and its data.

Personal Computers
It is not recommended that home computers are used for the production of KCC documents, particularly when individuals can be identified and the data about them may be sensitive. Personal PCs should only be used if they have up to date virus protection software installed on them, and only if no other members of the household have access to the PC. Any documents produced on home computers should be stored only on disk or USB devices such as memory sticks and not on the hard drive. If any information has been stored on the hard drive employees must ensure that the hard disk is reformatted, cleared using a suitable program or destroyed prior to selling the equipment. Disks or memory sticks used to produce documents at home may be brought into work and used on KCC computers provided they have been virus checked first.

Personal Email Facilities
Using a personal internet service provider to send documents to or from KCC is strongly discouraged although it is recognised that this is a practice that may be necessary in some circumstances. Personal or sensitive information should not be sent by email using personal email facilities to or from home as the security of the data cannot be guaranteed. The only exception to this is if it is necessary for the purpose of protecting a vulnerable person.

Employees must ensure that no other members of the household have access to their emails. The employee will be held personally responsible (under the Misuse of Computers Act) for any loss of confidential data from their PC or across the network.

Home Work Area Security
Incidental access to KCC data can be avoided by using appropriate precautions in the work area at home. PCs should be shut down when the work area is left unattended to ensure the system is secure at all times. When a PC or information is left unattended, doors/windows must be secured.

Manual information stored at home that identifies individuals must be kept in a locked facility if left unattended and should, under no circumstances be made available to or shared with anyone other than appropriate KCC employees. Manual information includes all paper files, printouts, correspondence, bank statements, etc., which identify individuals.

Transporting Data
When transporting client data between home and client premises, or between home and other locations, employees should take all reasonable steps to ensure that data security is maintained. For example, data should be transported in such a way as to minimise the opportunity of destruction or loss by ensuring vehicles used to transport the data are locked if left unattended and any passengers do not have access to it. Ideally information (including laptop computers that contain sensitive data) should always be transported in the boot of the vehicle and should not be left in unattended vehicles.

Disposal of Personal Information
Personal data should not be retained at home for longer than is necessary. Care should be taken when disposing of documents containing personal data at home. Such documents must be shredded or disposed of in such a way that prevents access by others. Placing data in a

waste bin is not a secure means of disposal and is unacceptable. If shredding facilities are not available at home then this should be done in a KCC office.

Privacy and Confidentiality

The Data Protection legislation requires those who record and use personal information to be open about that use and to follow sound and proper practices. All employees must be discreet with personal data at all times. This includes being aware that they have a responsibility to protect the privacy of individuals when holding conversations in public places, making telephone calls, sending faxes, etc. Any uses of personal information must be justified - therefore personal information must not be divulged to anyone who doesn't have a legitimate need to know and it must only be disclosed for authorised purposes.

Compliance with this guidance is essential for KCC employees who work at home as individuals can be held accountable for breaches of the Data Protection Act. Failure to ensure appropriate security of the data could place the organisations and the individual at risk of prosecution under the Data Protection Act 1998.