

Stratford-sub-Castle Church of England VC Primary School
Learning for life in a positive and caring Christian community

Data Protection Policy #2

The *Data Protection Policy and General Statement* was reviewed during the Autumn Term 2016.
This document is the result of that review.

DATE AGREED BY FULL GOVERNING BODY:	14/11/2016
REVIEW DATE:	2018/2019.
AUTHOR:	Mrs Kay Bridson & Mr Peter Habert
HEADTEACHER:	Mrs Kay Bridson
CHAIR OF GOVERNORS:	Miss Angela Britten
SIGNED:	
TO BE READ IN CONJUNCTION WITH:	<i>Aims of the School</i> <i>Single Equalities Policy</i> <i>Online-Safety Policy</i>

Stratford-sub-Castle Church of England VC Primary School

Learning for life in a positive and caring Christian community

Data Protection Policy #2

The Data Protection Policy and General Statement were reviewed during the Autumn Term 2016/2017. This document is the result of that review. It should be read in conjunction with the *Aims of the School, Single Equalities Policy and the Online-Safety Policy*.

This policy was agreed by the Full Governing Body on 14/11/2016

This policy will be reviewed in 2018/2019.

This document is a statement of the aims and principles of the school for ensuring the confidentiality of sensitive information relating to pupils, parents/carers, staff and governors.

Policy Summary

Introduction

Stratford-sub-Castle Church of England Primary School needs to keep certain information about our employees, pupils and other users to allow us, for example, to monitor performance, achievement and health and safety. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any person unlawfully. To do this, Stratford-sub-Castle Church of England Primary School must comply with the Data Protection Act 1998 (the Act).

The principles of the Act state that personal data shall be:

- obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- adequate, relevant and not excessive for that purpose
- accurate and kept up-to-date
- kept for no longer than is necessary for that purpose
- processed in accordance with the data subject's rights
- kept safe from unauthorised access, accidental loss or destruction.

All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff but it is a condition of employment that employees will abide by the rules and policies made by the school from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

- the school as a body corporate is the Data Controller under the Act and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day-to-day matters.

- the school has three Designated Data Controllers: They are the Headteacher, the Administration Officer and the Administration Assistant.
- any member of staff, parent/carer or other individual who considers that the Policy has not been followed in respect of personal data about themselves or their child should raise the matter with the appropriate Designated Data Controller who would be, in the first instance, the Administration Officer.

Responsibilities of Staff

All staff are responsible for:

- checking that any information that they provide to the school in connection with their employment is accurate and up-to-date.
- informing the school of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes.
- handling all personal data, e.g. pupil attainment data, with reference to this policy.

Data Security

All staff are responsible for ensuring that:

- any personal data that they hold is kept securely
- personal information is not disclosed either orally or in writing or electronically or by any other means, accidentally or otherwise, to any unauthorised third party.

Rights to Access Information

All staff, parents and other users are entitled to:

- know what information the school holds and processes about them or their child and why
- know how to gain access to it
- know how to keep it up-to-date
- know what the school is doing to comply with its obligations under the Act.

Retention of Data

The school has a duty to retain some staff and pupil personal data for a period of time following their departure from the school, mainly for legal reasons but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time according to need.

Monitoring and Evaluation

This is ongoing; where any clarifications or actions are needed these will be fed into the policy at its next review.

Data Protection Policy

General Statement

The Headteacher and Governors of Stratford-sub-Castle Church of England Primary School intend to comply fully with the requirements and principles of the Data Protection Act 1998.

All staff involved with the collection, processing and disclosure of personal data will be aware of the school's duties and responsibilities under the Data Protection Act 1998. Staff will be given training on the requirements of the Act as and when it is considered appropriate.

Enquiries

Information about the school's Data Protection Policy is available from the Headteacher and general information about the Data Protection Act can be obtained from Wiltshire County Council and the Information Commissioner's Office.

Fair Obtaining

The school undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for the collection of the data, the purposes for which the data is held, the likely recipients of the data and their right to access that data either under the Education (Pupil Information) (England) Regulations 2005 or the Data Protection Act 1998. Data subjects will be informed about the collection and use of their data through the use of Privacy Notices which will be printed on the appropriate collection forms. There is a general Privacy Notice which can be found on the school's website and a copy is attached as Appendix 1. If these details are given verbally to the data subject, the person collecting the data will explain the issues before obtaining the information.

Registered Purposes

The school's Notification with the Information Commissioner's Office (ICO) is available, by appointment, for inspection in the school office. The Notification includes the types of personal data the school holds and processes and the reasons for which the data is processed. Explanation of the codes and categories entered is available from the Headteacher. Information held for these stated purposes will not be used for any other purpose without the data subject's consent. The school's ICO Registration number is Z610224 and the School's Notification to the ICO can be found on the ICO's public register.

Data Integrity

The School undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances their record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate (challenged). We shall try to resolve the issue informally but if this is not possible, any disputes will be referred to the Board of Governors for their deliberation.

If the problem is not resolved at this stage independent arbitration may be sought by either side. Until resolved, the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information. In order to prevent such problem areas we shall provide data subjects with opportunities to check their data accuracy and request amendments.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive to the purpose for which the data is held. In order to ensure compliance with this principle, the Designated Data Controllers will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Designated Data Controllers to ensure obsolete data is properly erased.

Subject Access

The Data Protection Act extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Where a written request for subject access is received in respect of a pupil, the school's policy is that:

- requests from parents about the data held about their own child will, provided that the child is not of an age or ability to understand the nature of a subject access request, be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.
- requests from pupils who do NOT understand the nature of the request will be referred to the child's parents.
- requests from pupils who can demonstrate an understanding of the nature of their request will be processed as any subject access request as outlined below and the copy will be given directly to the pupil.

Processing Subject Access Requests

Pupils/parents should make a formal Subject Access request in writing to the Designated Data Controller.

Provided that there is sufficient information about the identity of the requester or their parent to process the request, an entry will be made in the *Subject Access Log Book*, indicating the date of receipt, data subject's name, name and address of requester (if different), type of data required (e.g. Pupil Record, Personnel Record) and planned date of supplying the information (not more than 40 calendar days from the request date).

Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

Authorised Disclosures

In general, the school will only disclose data about individuals with their consent. However, there are circumstances under which it is necessary for the school's Designated Data Controllers to disclose data the without express consent of the data subject.

These circumstances are limited to:

- Pupil data disclosed to authorised recipients in respect of education and administration necessary for the school to perform its legitimate duties and obligations.
- Pupil data disclosed to authorised recipients in respect of a pupil's health, safety and welfare.

- Data contained within a Pupil's educational record will be disclosed to the child's parents if requested in accordance with Educational (Pupil Information) (England) Regulations 2005.
- Staff data disclosed to the relevant authority in respect of payroll and school's staff administration
- Other disclosures as may prove unavoidable, for example where an incidental disclosure occurs when an engineer is fixing the computer systems. In such cases, the engineer will sign a document to undertake NOT to disclose such data outside the school. Local Authority IT Liaison/Support Officers are professionally bound not to disclose such data.

Only authorised and properly instructed staff are permitted to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare workers must be made available only if the staff member needs to know the information for their work within the school.

Data and Computer Security

The school undertakes to ensure security of personal data by the following general methods – (for security reasons we cannot reveal precise details in this document):

Physical Security

Appropriate building security measures are in place, such as alarms and lockable cabinets. Printouts, digital storage devices and files are locked away securely when not in use. Visitors to the school are required to sign in and out and are, where appropriate, accompanied.

Logical Security

Security software is installed on all computers containing personal data, only authorised users are allowed access to the computer files and password changes are regularly undertaken. Digital personal data is encrypted or password-protected both on a local hard drive and on a network drive that is regularly backed up. If personal data is kept on a USB memory stick or other removable storage media, that media must itself be encrypted/password protected and/or kept in a locked filing cabinet, drawer or safe. Filing cabinets should be kept locked when the room is unattended.

The school has an electronic 'cloud' space. Within this space there are various SharePoint areas for teachers and governors with access to documents. Access to the SharePoint areas are managed by the administrator for that area who can choose who can view and/or edit files. SharePoint areas should be used to store documents, therefore documents should not be saved on personal electronic devices.

As well as the SharePoint areas, the school electronic 'cloud' space has an area called OneDrive which is for the individual only to use. Documents saved on the OneDrive space should only be related to school matters.

Procedural Security

In order to be given authorised access to the computer, staff will be properly checked and will sign a confidentiality agreement. All staff are trained and instructed in their Data Protection obligations and their knowledge updated as necessary. Computer printout and source documents containing personal data are always shredded before disposal.

Overall security policy is determined by the Headteacher and will be monitored and reviewed as appropriate and whenever a major security breach or loophole is apparent. The school's security policy is kept in a safe place at all times. Any queries or concerns about security of data within the school should be brought to the attention of the Headteacher.

Emails

Each member of staff and governor is provided with a school email address to use only for school business. When a member of staff or governor leaves, their email account will be deleted. Personal email accounts should not be used by staff or governors for school related business.

Staff and Governor email accounts allow individuals to access SharePoint areas. Therefore, once email accounts are deleted individuals can no longer access SharePoint areas.

Individual members of staff can be liable in law under the terms of the Act. They may also be subject to damages claims from persons harmed as a result of inaccuracy, unauthorised use or disclosure of their data. Any deliberate breach of this Data Protection Policy will be treated as a disciplinary matter and serious breaches may lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from the school.

Appendix 1

Privacy Notice - Data Protection Act 1998

We Stratford-sub-Castle Church of England Primary School are the Data Controller for the purposes of the Data Protection Act 1998. We collect information from you, and may receive information about you from your previous school. We hold this personal data and use it to:

- support your teaching and learning
- monitor and report on your progress
- provide appropriate pastoral care, and
- assess how well your school is doing

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some of your information to the Local Authority (LA), and the Department for Education (DfE).

If you want to see a copy of the information we hold and share about you then please contact Mrs Kay Bridson, the Headteacher.

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

<http://www.wiltshire.gov.uk/dce-la-privacy-notice-v2-feb2016.pdf>

<https://www.gov.uk/government/organisations/department-for-education>