Stratford-sub-Castle Church of England VC Primary School

Learning for life in a positive and caring Christian community

Data Protection Policy #3

The *Data Protection Policy and Privacy Notice* were reviewed during the Spring Term 2018 in-line with the new obligations under the General Data Protection Regulations.
This document is the result of that review.

DATE AGREED BY FULL GOVERNING BODY:	**26/03/2018**
REVIEW DATE:	**November 2020**
AUTHOR:	**Mrs Kay Bridson & Mr Peter Habert**
HEADTEACHER:	**Mrs Kay Bridson**
CHAIR OF GOVERNORS:	**Miss Angela Britten**
SIGNED:	
TO BE READ IN CONJUNCTION WITH:	***Aims of the School*** ***Privacy Notice*** ***Use of Photography and Images Policy*** ***Acceptable Use Policy*** ***Child Protection Policy*** ***Freedom of Information and Publications Policy*** ***Information Sharing Policy*** ***Safeguarding Policy***

Stratford-sub-Castle Church of England VC Primary School

Learning for life in a positive and caring Christian community

Data Protection Policy #3

1. Our Commitment

Stratford-sub-Castle Church of England VC Primary School (the School) is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles promoted by the Information Commissioners Office (ICO) and current regulations. Changes to data protection legislation (General Data Protection Regulation, from 25 May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The school is also committed to ensuring that its staff are aware of their responsibilities under this policy and the law through regular training. The members of staff responsible for data protection are [DATA PROTECTION OFFICER (DPO)/ HEADTEACHER/ SCHOOL ADMINISTRATOR].

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

2. Data Controller

The School as a body corporate is the Data Controller and its data processing activities are registered with the ICO. Details are available on the ICO's public register. The School's ICO Registration number is Z610224, and the School's 'Privacy Notice' (located in Appendix 1) is also included on the School's website.

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

3. Data Protection Principles

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

When processing personal date, the School will adhere to the principles which set out the main responsibilities for organisations (Article 5 of the GDPR), that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. The Lawful Basis for Processing Data

The lawful basis for the School processing data (under Article 6 of the GDPR) have been identified as follows:

(a) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.

(c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations)

(e) Public task: the processing is necessary for the School to perform its official functions

Members of staff will ensure that at least one of these basis will apply whenever personal data is processed. If no lawful basis is identified, personal data will not be processed.

5. Authorised Disclosures

In most circumstances the School will be required by 'contract', 'legal obligation' or 'public task' to pass personal data on to external authorities (for example local authorities, OFSTED and the Department for Education (DfE). In these circumstances, the School is not required to seek specific consent.

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 an agreement to 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.

Examples of Authorised Third Party Disclosures:

***Other schools**:* If a pupil transfers from the School to another school, their academic records and other data that relates to their health and welfare will be forwarded to the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

Examination authorities: This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

***Health authorities**:* As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts: If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

Social workers and support agencies: In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

***Educational division**:* Schools may be required to pass data on in order to help the local authority and the government to monitor the national educational system and enforce laws relating to education.

6. Where Consent Is Required

Where the School has deemed that the lawful basis for processing personal data is 'consent', the School will make its consent request prominent, concise and easy to understand. The request will include:

- the School's name;
- the name of any third party controllers who will rely on the consent;
- why the School wants the data;
- what the School will do with it; and
- explain that individuals can withdraw consent at any time.

The School's consent request will not use pre-ticked boxes, opt-out boxes or other default settings.

The School will keep records to evidence consent (who consented, when, how, and what they were told) and make it easy for people to withdraw consent at any time they choose.

Consents will be kept under review and refreshed if anything changes.

7. Privacy by Design (Data Protection Impact Assessments)

To assure the protection of all data being processed and inform decisions on processing activities, the School shall undertake Data Protection Impact Assessments (DPIA) of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

A DPIA will be carried out in line with the ICO's Code of Practice for Conducting Privacy Impact Assessments when:

- using new technologies
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

The School's DPIA form is included in Appendix 2.

8. Data and Computer Security

Security of data shall be achieved through consideration of the DPIA and the subsequent implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

The School undertakes to ensure security of personal data by the following general methods:

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.

Digital 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's 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.

Email Accounts
Each member of staff and governor is provided with an 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.

Any deliberate breach of this Data Protection Policy will be treated as a disciplinary matter and serious breaches may lead to dismissal.

9. Subject Access Requests

All individuals whose data is held by us, have a legal right to request access to such data or information about what is held.

No charge will be applied to process the request (however, a reasonable fee will be charged at the discretion of the School if the request is unfounded or excessive, particularly if repetitive).

Personal data about pupils will not be disclosed to unauthorised third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child.

10. Processing Subject Access Requests

Pupils/parents should make a formal Subject Access request in writing to the [Data Protection Officer/School Administrator/Head Teacher].

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 20 calendar days from the request date).

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

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.

- from pupils who do NOT understand the nature of the request will be referred to the child's parents.

- 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.

11. Right to be Forgotten

The School recognises that where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

12. Photographs and Video

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources. It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent and should not then share these images on any form of social media (including but not limited to: Facebook, Instagram, Twitter, Snap Chat, WhatsApp, LinkedIn etc). Further details can be found in the Use of Photography and Images Policy.

13. Data Disposal

The School recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The school has identified a qualified source for disposal of IT assets and collections.

14. Data Protection Breaches

The GDPR imposes a duty on the School to report certain types of personal data breach to the ICO.

When a personal data breach has occurred, the DPO and the Headteacher will establish the likelihood and severity of the resulting risk to people's rights and freedoms.

If it's likely that there will be a risk then the School's DPO will notify the ICO within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the School will also inform those individuals without undue delay.

If it is likely that the breach will not pose a risk, the School may decide not report the breach to the ICO. In such circumstances the School will justify and document its decision.

The School's DPO will keep a record of all personal data breaches.

Appendix 1

Privacy Notice (how we use pupil information)

We Stratford-sub-Castle Church of England Primary School are the Data Controller for the purposes of the Data Protection Act.

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- Special educational needs information
- Exclusions / behavioural information

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess how well the school is doing
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013 and for data collection purposes under the Education Act 1996 – this information can be found in the census guide documents on the following website https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data for [settings need to include the length of time for which the personal data will be stored]

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority

- the Department for Education (DfE)

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the headteacher

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact the headteacher

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, the please go to the following websites:

http://www.wiltshire.gov.uk/privacy
http://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

Pip Rabbitts Data and Information Sharing Manager Wiltshire Council Bythesea Road Trowbridge BA14 8JN	Public Communications Unit Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT
Pip.rabbitts@wiltshire.gov.uk	http://www.education.gov.uk/help/contactus
01225 713091	0370 000 2288

Appendix 2

Data Protection Impact Assessment Form

Project/Technology/Risk Assessed:	
Date of Assessment:	
Assessment Completed By:	

A) Description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller (the School).

B) Assessment of the necessity and proportionality of the processing in relation to the purpose.

C) Assessment of the risks to individuals.

D) The measures in place to address any risk, including security.

E) Does this DPIA address more than one project?
