Whitchurch Church of England Primary School **Policy and Procedure Statement**	Effective Date:	May 2018
Together we make a difference With love, courage and respect **Data Handling** **Policy & Procedure** General Data Protection Regulations 2018 (GDPR)	Revision Date:	May 2020
	Page No:	1 of 4
	Approval:	
Head Teacher	Mrs K Steven	
DSL	Mrs K Steven	
Chair of Governors	Mrs C Datta	

1.0 Scope

A key principle of the General Data Protection Regulations GDPR is that personal data should be processed securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

Article 5(1)(f) of the GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall be:

'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'

2.0 Responsibility and definitions

The Governing Body – is the Data Controller and has overall responsibility for the School's data ecosystem, policies and compliance with GDPR;

The Headteacher – is the school's senior leader and is responsible on a day to day basis with the SLT for overall GDPR compliance on behalf of the Governing Body;

The DPO is responsible for supporting the Headteacher and Governing Body to ensure compliance by reviewing Data Handling Procedures and auditing compliance with Data Protection Legislation.

3.0 Policy & Procedure

3.1 Data Protection Policy

All staff should read and understand the Data Protection Policy. A copy is available on DB or from the school office and on the school website. Data Protection training will be carried out at the annual INSET training in September each year and form part of new staff induction.

3.2 Subject Access Requests

Everyone has the right to access information held on them, regardless of the medium in which it is held i.e. electronically or on paper. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request. Should you receive a request to provide information please refer this directly to the Data Protection Officer. We must fulfil these requests within one month.

3.3 Data Breach

Systems are in place to help reduce the risk of a data breach e.g. personal data sent out checked before the envelope sealed, uploads to websites checked, email trails, attachments to emails and recipients addresses checked before sending etc. If you become aware that there has been a data breach, however minor, this must immediately be brought to the attention of the Data Protection Officer who will assist in ensuring we understand what has occurred, respond to the incident, ensure the breach is contained and report it if necessary. This must be done within 72 hours of becoming aware of the breach. Please also refer to our Data Breach Procedures for further information.

3.4 Data Retention & Storage

Personal data will be held securely and must not be held for any longer than is necessary to fulfil the need for which is was originally intended.

Paper based documents will be held securely and a clear desk policy, in relation to personal or sensitive information, will be maintained at all times.

3.5 Data Destruction

Records will be destroyed in accordance with HCC Records Retention Policy. All personal and sensitive data will be destroyed as confidential waste (shredded) or deleted securely from electronic systems.

4.0 Systems to protect data

4.1 ICT Systems

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

4.2 Personal Data

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed).

Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

The school has procedures for automatic backing up, accessing and restoring all data held on school systems, including off-site backups – Agile ICT.

4.3 Portable Devices

All portable devices containing personal data are password protected i.e. Teacher iPads. All staff have access to remote working where necessary. This gives access to all school files. Memory sticks will not be used to transport or store personal data.

When personal data is stored on any portable computer system, iPAD or any other removable media the device must be password protected and the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

4.4 Images

Images of pupils and staff will be protected and stored securely on the school system. The school will ensure we have explicit permission to use/share images. Permission for this will be obtained in the Photographic and Media Consent Form issued to all parents.

4.5 Passwords

Staff will make use of complex passwords for computer equipment, websites, password protected documents etc. Using a different password for every website that is long and has multiple types of characters (numbers, letters, and symbols). It is advisable NOT to record complete passwords, but prompts could be recorded. Passwords must be changed regularly and must not be shared between staff

4.6 Third Party data transfers

As a Data Controller, the school is responsible for the security of any data passed to a third party. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party as well as data processing agreements. We will state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR.

4.7 Paper Based Systems

All paper based personal data will be protected by appropriate controls, to include:

- Paper based safeguarding chronologies will be in a locked cupboard when not in use, with keys kept by authorised personnel
- Class Lists used for the purpose of marking may be stored in a teacher's bag
- Class Files are marked confidential and will be locked away at the end of the school day
- Paper based personal information sent to parents will be checked before the envelope is sealed.
- Paper based pupil contact sheets will be stored in a lockable cupboard
- Paper based staff contact sheets will be stored in a lockable cupboard
- Pupil Files, Personnel Files, SEN Files etc are stored in a locked filing cabinet when not in use, with keys kept by authorised personnel

- Financial Records are kept in a locked cupboard when not in use, with keys kept by authorised personnel

4.8 School Website

Uploads to the school website will be checked prior to publication:

- to check that appropriate photographic consent has been obtained
- to check that the correct documents have been uploaded

4.9 E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

Where technically possible all e-mail containing sensitive information will be encrypted by attaching the sensitive information as a word document and encrypting the document/ compressing with 7 zip and encrypting. The recipient will then need to contact the school for access to a one-off password

Staff will be careful with identifying content within e-mails. If people/pupils are named it becomes specific to them and they can ask to see it. When seeking advice, it is better, where possible, to refer to a pupil in a year group rather than name a specific child.

Staff must not auto forward emails from their school email address to a private email address.

5.0 Dealing with Sensitive Data

- The school must not send potentially sensitive information to the wrong parent and should seek advice immediately if this happens
- If it is essential to take data off site staff must secure it in transit and in storage away from base. Lockable document bags are provided when it is necessary to transport documents offsite e.g. to an Early Help Hub Meeting.
- Staff need to be careful with identifying content within e-mails. If people/pupils are named it becomes specific to them and they can ask to see it. When seeking advice it is better, where possible, to refer to a pupil in a year group rather than name a specific child
- Sensitive data includes information about child protection, medical information, SEN, finance, personnel data. Where possible it is advisable is to encrypt sensitive data.
- When requests for copies of data are made by parents, these should preferably be in writing. Staff must date the requests when received as a time frame must be followed. Schools will keep an exact copy of what is provided to parents – including both redacted and non-redacted information. Further information is available within the SAR Procedures.