The Parish of

St Mary the Virgin

STANWELL

&

St Matthew

ASHFORD

Data Protection Policy

1. Aim

The Parochial Church Council (PCC) aims to ensure that all Personal Data collected, stored, processed and destroyed by any natural person – whether they be a member of staff, a member, a visitor, a contractor, a consultant, or any other individual – is done so in accordance with the DPL, case law and any other statute.

This policy applies to all Personal Data collected, stored, processed and destroyed by the PCC or one of its groups, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in and whether the collection of Processing of data was, or is, in any way automated.

2. Legislation and guidance

This policy meets the requirements of the DPL. It is based on guidance published by the ICO.

The policy meets the requirements of the Protection of Freedoms Act 2012, ICO's Code of Practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information.

3. Definitions

Term	Definition
'PCC'	Refers to the Parochial Church Council.
'CCTV'	Refers to Closed Circuit Television.
'Consent'	Freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
'Data Breach'	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.
'Data Controller'	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

'Data Processor'	A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller, following the Controller's instructions.
'Data Subject'	The identified or identifiable individual whose Personal Data is held or processed.
'DBS'	Refers to the Disclosure and Barring Service.
'DPL'	Refers to data protection law, including the EU's General Data Protection Regulation, the Data Protection Act (as revised from time to time), case law, regulations, and statutory guidance.
'DPO'	Refers to the Data Protection Officer.
'FBP'	Finance Buildings and Personnel Committee
'HMRC'	Refers to Her Majesty's Revenue and Customs Office.
'ICO'	Refers to the Information Commissioners' Office.
'Personal Data'	Any information relating to an identified or identifiable natural or legal person (e.g. a Data Subject); an identifiable natural or legal person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as: • A name; • An identification number; • Location Data; • An online identifier; and / or • One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural or legal person.
'Processing'	Any operation, or set of operations, which is performed on Personal Data, or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

	dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing can be automated or manual.
'Special Categories of Personal Data'	Personal Data which is more sensitive and so needs more protection. Such data includes information about an individual's: • Racial or ethnic origin; • Political opinions; • Religious or philosophical beliefs; • Trade union memberships; • Genetics; • Biometrics (i.e. fingerprints, retinal or iris patterns), where used for identification purposes; • Health (including physical and mental); • Sexual history or sexual orientation; and / or • History of offences, convictions or cautions*. * Whilst criminal offences are not classified as 'sensitive data' within the Data Protection Act 2018, the Trust has included it within this policy as acknowledgement of the care needed with this data set.

4. The Data Controller

The PCC, in all of its work, processes Personal Data relating to members, staff, visitors and others, and, therefore, is a Data Controller and a Data Processor.

5. Roles and responsibilities

This policy applies to all staff employed by the PCC and to all external organisations or individuals working for the PCC or on the PCC's behalf. Non-compliance with this policy may result in action being taken by the PCC.

5.1. The PCC

The PCC have overall responsibility for ensuring that the Parish comply with all the relevant data protection obligations. The PCC will seek to

perform its responsibility by reviewing this policy regularly, appointing a DPO and delegating the responsibility to implement this policy to the FBP.

5.2. The Data Protection Officer

The PCC have appointed Mrs Julie Bell as it's Data Protection Officer, who can be contacted via email at treasurer@smam.org.uk

The DPO is responsible for overseeing the implementation of this policy in the first instance, before reviewing the PCC's compliance with the data protection law and developing related policies and guidelines where applicable.

The DPO will provide an annual report of compliance and risk issues directly to the PCC with recommendations and advice.

The DPO will be the named point of contact for individuals whose data the PCC processes.

5.4. The Senior Parish Administrator

The Senior Parish Administrator acts as the representative of the Data Controller on a day-to-day basis.

5.5. Staff

All staff (regardless of role) are responsible for:

- Collecting, storing, and Processing any Personal Data in accordance with this policy;
- Informing the PCC of any changes to their Personal Data (i.e. a change of address, telephone number, or bank details); and
- Reporting a Data Breach, Data Right Request or Freedom of Information Request.
- Contacting the DPO:
    - With any questions about the operation of this policy, data protection law, retaining Personal Data, or keeping Personal Data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether or not they have a lawful basis to use the Personal Data in a particular way;
    - If they need to rely on, or capture Consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer Personal Data outside of the European Economic Area;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals; and

- If they need help with any contracts or sharing Personal Data with third parties.

6. The Principles of Data Protection Law

The EU's General Data Protection Regulation is based on seven data protection principles that the PCC must comply with; these require that all data be:

- Processed lawfully, fairly, and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which is it is processed; and
- Processed in a way that ensures it is appropriately secure.

The accountability principle ties these together by requiring an organisation to take responsibility for complying with the principles, including having appropriate measures and records in place to be able to demonstrate compliance.

This policy sets out how the PCC aims to comply with these key principles.

7. Collection of Personal Data

7.1. Lawfulness, fairness and transparency

The PCC will only process Personal Data where it has met one of the six lawful reasons to do under the Data Protection Act 2018. The six lawful reasons are that:

- The individual (or their parent / carer in the case of a child/vulnerable adult, where appropriate) has freely given clear **Consent;**
- The data needs to be processed so that the PCC can **fulfil a contract** with the individual, or the individual has asked the PCC to take specific steps before entering into a contract;
- The data needs to be processed so that the PCC can **comply with a legal obligation**;
- The data needs to be processed to ensure the **vital interests** of the individual (i.e. to protect someone's life);
- The data needs to be processed so that the PCC, can perform a **task in the public interest,** and carry out its official functions; and / or

- The data needs to be processed for the **legitimate interests** of the parish or a third party (provided the individual's rights and freedoms are not overridden).

For Special Categories of Personal Data, the PCC will need to meet one of the special category conditions for Processing as set out in the Data Protection Act 2018. The conditions are when:

- The individual (or their parent / carer in the case of a pupil, where appropriate) has given **explicit Consent;**
- It is necessary for the purposes of carrying out the **obligations and exercising specific rights** of the controller or of the data subject in the field of **employment** of a Data Controller or of a Data Subject;
- It is necessary to protect the **vital interests** of the Data Subject;
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
- The Personal Data has **manifestly been made public** by the Data Subject;
- There is the **establishment, exercise or defence of a legal claim**;
- There are reasons **of public interest** in the area of **public health**;
- Processing is necessary for the purposes of preventative or occupational medicine (e.g. for the **assessment of the working capacity of the employee**, the medical diagnosis, the provision of health or social care or treatment); and / or
- There are **archiving** purposes in the **public interest**.

If the PCC decides to offer online services to members, such as classroom applications, and the PCC intended to rely on Consent as a basis for Processing, the PCC will need to get parental consent for this (except for online counselling and preventative services).

Where the PCC collect personal data directly from individuals, the PCC will provide them with the relevant information required by data protection law, in the form of a privacy notice.

Hard copies of the Privacy Notices are available on request by contacting the Administrator for the PCC.

7.2. Limitation, minimisation and accuracy

The PCC will only collect Personal Data for specific, explicit and legitimate reasons. The PCC will explain such reasons to the individuals (or their

parents / guardians, where appropriate) when the PCC first collects their data in accordance with the PCC's privacy notices.

If the PCC wishes to use the Personal Data for reasons other than those given when the data was first obtained, then the PCC will inform the individuals concerned before doing so and seek further Consent where necessary.

Staff must only process Personal Data where it is necessary in order to fulfil their designated duties.

When Personal Data is no longer required, staff must ensure that it is deleted. This will be done in accordance with the Document Retention Schedule, which states how long a particular type of document may be kept and how it should be destroyed.

Copies of the Document Retention Policy can be obtained by contacting the Administrator.

8. Sharing Personal Data

In order to efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but not limited to;

- There is an issue with a someone that puts the safety of PCC's staff at risk; or
- The PCC needs to liaise with other agencies or services (the PCC pledges to seek Consent, as applicable, prior to sharing Personal Data in relation to this);
- The PCC's supplies or contractors need data to enable the PCC to provide services to staff and members (i.e. information technology companies). The PCC pledges that when sharing data, in this relation to this, it will:
    - Only appoint suppliers or contractors who can provide sufficient guarantees that they are in compliance with the data protection laws and have satisfactory security measures in place;
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful Processing of any Personal Data it shares; and
    - Only share data that the supplier or contractor needs to carry out their service and any such information necessary to keep them safe while working with the PCC.

The PCC will also share Personal Data with law enforcement and government bodies where it is under a legal obligation to do so, such as:

- The prevention or detection of crime and / or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to the HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy the PCC's safeguarding obligations; and
- For research and statistical purposes, as long as the PCC is satisfied that the Personal Data shared will be sufficiently anonymised or Consent from the Data Subject has been obtained.

The PCC may also share Personal Data with emergency services and local authorities to help them response to an emergency situation affecting the congregants or staff.

In the event that the PCC transfers Personal Data to a country or territory outside of the European Economic Area, it will do so in accordance with data protection laws and will consult with the affected Data Subjects first.

9. Individual rights

9.1. Subject access requests

Data Subjects have a right to make a 'subject access request' to access any Personal Data held by the PCC about them. This includes:

- Confirmation that their personal data is being processed;
- Access to a copy of the data;
- The purposes of the data processing;
- The categories of personal data concerned;
- Who the data has been, or will be, shared with;
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- The source of the data, if not the individual; and / or
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

While the PCC will comply with the General Data Protection Regulation when dealing with subject access requests submitted in a written form. Data Subjects are requested to submit their subject access requests by letter, email, or fax, addressed (or marked) for the attention of the DPO. All requests must include:

- The name of the Data Subject;
- A correspondence address;
- A contact number;
- An email address; and
- Details of the Personal Data requested.

In the event that a subject access request is submitted to a member of PCC's staff, it should be immediately forwarded to the DPO

9.2. Responding to subject access requests

When responding to requests, the PCC:

- May request the Data Subject to provide two forms of identification from the list below:
    - Passport,
    - Driving licence,
    - Utility bills with the current residential address of the Data Subject,
    - P45 / P60, and
    - Credit card or mortgage statement;
- May contact the Data Subject via phone to confirm the request;
- Will respond without delay and within 1 month of receipt of the request;
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this as soon as possible and explain why the extension is necessary.
- Will provide the information free of charge (unless it is found to be onerous, excessive or unfounded). Any fee charged will be reasonable and would only account for the administrative costs incurred while complying with the request.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of an individual; or
- Would reveal a child/vulnerable adult is at risk of abuse, where the disclosure of that information would not be in the child/vulnerable adult's best interests; or
- Is contained in adoption or parental order records; or
- Is given to a court in proceedings concerning a child/vulnerable adult.

If the request is manifestly unfounded or excessive, we may refuse to act on it, or charge a fee as explained above.

A request will be deemed to be manifestly unfounded or excessive if it is repetitive or asks for further copies of the same information.

In the event the PCC refuse a request, we will tell the individual why, and tell them they have the right to refer a complaint to the ICO.

9.4. Other data protection rights of the Data Subject

In addition to the right to make a subject access request and to receive information when the PCC is collecting the data and about how the PCC uses and processes the data; Data Subjects also have the right to:

- Withdraw their consent to processing at any time, this only relates to tasks which the parish relies on consent to process the data;
- Ask the PCC to rectify, erase, or restrict Processing of the Data Subject's Personal Data, or object to the Processing of it in certain circumstances;
- Prevent the use of any Personal Data for direct marketing;
- Challenge Processing which has been justified on the basis of public interest;
- Object to decisions based solely on automated decision making or profiling (e.g. decisions taken with no human involvement that might negatively affect them);
- Be notified of a Data Breach in certain circumstances;
- Make or lodge a complaint with the ICO; and / or
- Ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Data Subjects should submit any request to exercise these rights to the DPO

If staff receive such a request, they must immediately forward it to the DPO

10. Closed Circuit Television

The PCC uses CCTV in various locations around the various buildings for the prevention and detection of crime. However, footage may be used for additional reasons specified more fully in the CCTV Policy. The PCC adheres to the ICO's Code of Practice for the use of CCTV. Any enquiries about the CCTV system used by the PCC should be directed to the DPO.

The PCC does not need to ask individuals' permission to use CCTV, but makes it clear where individuals are being recorded with security cameras, which are clearly visible and accompanied by prominent signs explaining

that CCTV is in use, where not clear, directions will be given on how the individual may obtain further information.

The full CCTV policy can be found by requested from the office. Any enquiries about the CCTV system should be directed to the DPO.

11. Photographs and videos

As part of church activities, the PCC may take photographs and record images of individuals within the PCC's buildings and grounds.

The PCC uses photographs:

- Within the PCC's churches on notice boards and in magazines, brochures, newsletters and prospectuses; and Online on the PCC's website or social media pages.

The PCC will clearly explain how photographs and or video will be collected and used when obtaining consent.

Consent can be refused or withdrawn at any time. If Consent is withdrawn, the PCC will endeavour to delete the photograph or video and will not distribute it further.

Consent can be withdrawn by writing to the Parish Office.

When using photographs and videos of children in this way, the PCC will not accompany them with any other personal information about the child to ensure that the child cannot be identified.

12. Data protection by design and default

The PCC will put measures in place to show that the PCC has integrated data protection into all of its data collection and processing activities. These include, but are not limited to, the following organisational and technical measures:

- Only Processing Personal Data that is necessary for each specific purpose of Processing and always in line with the data protection principles set out in the relevant data protection regulations;
- Integrating data privacy impact assessments where the PCC's Processing of Personal Data presents a high risk to the rights and freedoms of Data Subjects and when introducing new technologies or Processing tools, in such cases advice will be sought from the DPO;
- Integrating data protection into internal documents including this policy and any related policies and privacy notices;
- Periodic reviews and audits to test the PCC's privacy measures and make sure that the PCC remains compliant; and

- Maintaining records of the PCC's Processing activities, including:
    - Making available the name and contact details of the PCC and the PCC's DPO and all information the PCC is required to share regarding its use and Processing of Personal Data (via the PCC's Privacy Notices) – for the benefit of Data Subjects; and
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

The PCC will protect all Personal Data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular, the PCC's organisational and technical measures include:

- Keeping paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain Personal Data under lock and key when not in use.
- Not leaving papers containing Personal Data on office desks, pinned to notice / display boards, or left anywhere else where there is general access.
- Passwords that are at least eight (8) characters long containing letters and numbers are used to access parish computers, laptops and other electronic devices. Staff and volunteers should be reminded to change their passwords at regular intervals.
- Encryption software is used to protect any devices such as Laptops, Tablets and USB Devices where saving to the hard drive is enabled.
- Staff, volunteers or PCC officers who store personal data on their personal devices are expected to follow the same security procedures as for parish-owned equipment (please refer to the PCC's ICT User Agreement – Appendix A).
- Where the PCC needs to share personal data with a third party, the PCC will carry out due diligence and take all reasonable steps to ensure that Personal Data shared will be stored securely and protected adequately.

14. Disposal of records

Personal Data that is no longer needed will be disposed securely. Personal Data that has become inaccurate or out of date will be disposed securely, in the instance where the PCC does not need to rectify it or update it.

For instance, the PCC will shred paper-based records and overwrite or delete electronic files. The PCC may also use a third party to safely dispose records on the PCC's behalf. In this instance, the PCC will require the third party to provide sufficient guarantee that it complies with the data protection law and a certificate of destruction, which will be recorded on to the PCC's systems.

When records are disposed of as part of the Data Retention schedule this is then recorded on our record of destruction log.

15. Personal Data breaches

The PCC will make all reasonable endeavours to ensure that there are no Personal Data breaches. In the unlikely event of a suspected Data Breach, the PCC will follow the procedure as set out in the PCC's Breach Management Policy.

All potential or confirmed Data Breach incidents should be reported to the Parish Priest and PCC Secretary where they will be assigned a unique refence number and recorded in the parish's data breach log.

Once logged, incidents will then be investigated, the potential impact assessed, and appropriate remedial action undertaken. The DPO will be consulted as required.

Where appropriate, the PCC will report the data breach to the ICO and affected Data Subjects within 72 hours.

The full procedure is set out in the PCC's Breach Management Policy, which can be requested from the parish office.

Examples of a Data Protection Breach include but are not limited to:

- Personal data being left unattended;
- Sending information to the wrong recipient;
- A non-anonymised dataset being published;
- Safeguarding information being made available to an unauthorised person; and / or
- The theft of a parish laptop containing non-encrypted personal data about volunteers.

16. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work, they carry out.

The DPO will work with Finance, Buildings and Personnel Committee and the Senior Parish Administrator to ensure that this policy remains contemporaneous and appropriate.

This policy will be reviewed every two years.

Appendix A - ICT User Agreement

1. Scope

This Agreement applies to all individuals who volunteer, are employed, or are contracted by the PCC. Please note that the above list is not exhaustive.

This Agreement covers the use of all digital technologies while on PCC premises (including, but not limited to, the use of e-mails, internet, intranet, network resources, learning platforms, software, communication tools, social networking tools, parish website, applications on portable electronic devices and other relevant digital systems provided by the PCC.

Additionally, this Agreement covers:

- The use of any PCC issued equipment (as logged on the Asset Register) when used outside of the PCC's building's.
- The use of any online systems provided by the PCC (including, but not limited to, VPNs and webmail);
- Any internet posts posted or made by individuals connected to the PCC on any non-PCC official social media platforms or applications which references the PCC or its buildings which might cause harm to the professional reputation of the PCC or any persons connected to the PCC.

The PCC regularly reviews all User Agreements and Privacy Notices with the assistance of the Data Protection Officer so that they are consistent with the current PCC policies.

The PCC have appointed Mrs Julie Bell as it's Data Protection Officer, who can be contacted via email at treasurer@smam.org.uk

2. The Agreement

I will only use the PCC's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the FBP.

3. Acceptable ICT resources and systems usage

Instances of receiving questionable material, or chancing upon an undesirable website, must be reported to the Parish Priest and Wardens immediately.

- Emails sent to an external organisation must be written carefully and checked before sending in the same way as a letter written on headed

paper. Avoid the autofill facility and check recipients before sending to ensure information remains secure.

- Encrypt or password protect any document containing sensitive information before sending it to any recipient. Agree the password code via another communication method – phone, text as appropriate.
- Keep personal details safe and do not give them out over the internet.
- Everyone must develop and maintain their knowledge of internet safety issues, particularly with regard to how they might affect children.
- The PCC will only obtain internet services from approved Internet Service Provider.
- Change passwords once every term to a "strong" password which includes capital letters, lower case letters, numbers and symbols with a minimum of eight characters.
- Ensure that the password auto save function on computers and personal laptops is turned off.
- Ensure all documents, data, etc. are printed, saved, accessed, deleted, and shredded in accordance with the PCC's network and security protocols and the PCC's Data Retention Schedule.
- Use the online Learning Platform or online cloud storage service in accordance with the provider's protocols and this Agreement.

4. Unacceptable ICT resources and systems usage

- It is not acceptable to access, transmit or create any offensive, obscene or indecent images, sounds, data or other material, as well as material that is defamatory, violent, abusive, racist, homophobic, extremist in nature or that may cause needless anxiety.
- Bringing the name of the PCC into disrepute
- Breach of confidentiality that results in information being inappropriately made available to others, including through social networking sites used from phones and home computers.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 2018.
- Transmission of commercial or advertising material or access to gambling websites.
- Violate the Data Protection Act 2018 by deliberately corrupting or destroying other users' data or violating privacy of others.

- Disrupting the work of others or wasting the time of staff or other users.
- Do not upload a photo to your email profile.

This is not an exhaustive list. The PCC reserves the right to amend this list at any time. The Parish Priest and Wardens will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the PCC's ICT facilities. Staff/Volunteers who engage in any of the unacceptable activity listed above may lose access to the system(s).

5. Access to ICT facilities and materials

The FBP manage access to the PCC's ICT facilities and materials for PCC staff / volunteers. That includes, but is not limited to:

- Computers, tablets and other mobile devices;
- Access permissions for certain programmes or files; and / or the
- Use of copier facilities.

Personal use of ICT facilities is acceptable, including copying, but must not be overused or abused.

Only devices supplied or authorised by the PCC must be used to access the parish network, as the FBP will have ensured that they meet the required level of security and protection hardware and software.

Authorised users will be provided with unique log-in / account information and passwords that they must use when accessing the ICT facilities, these must not be shared or borrowed. "One user, One login."

Individuals who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, must contact the Parish Priest or Wardens.

7. Use of email

Parish emails must only be used for official purposes.

Any information downloaded when remote working onto a personal device must be deleted upon the completion of the task.

Staff / volunteers must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Users must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to Subject Access requests from individuals under the Data Protection Act 2018 in the same way as paper documents.

Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages must be treated as potentially retrievable, therefore take extra care when composing them.

Individuals must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information, or the data of multiple individuals must be encrypted so that the information is only accessible by the intended recipient.

If users receive an email in error, the sender must be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the (Executive) School Business Manager immediately and follow the PCC's data breach procedure.

8. Use of phones

Parish phones must not be used for personal matters.

Individuals who are provided with the use of a mobile phone as equipment for their role must abide by this Agreement.

If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so.

The PCC does not permit taking photos or videos of children on personal devices. Where photos are taken at staff social events, these must not be published without the express agreement of the people involved.

The PCC's workforce must never send, or accept from anyone, texts or images that could be viewed as inappropriate.

All parish email users must ensure their phones are protected with appropriate password codes in case of loss or theft.

6. Social media

The PCC's workforce will ensure that any private social networking sites / blogs, etc. that they create or actively contribute to are not confused with their professional role and must create a clear distinction between the two.

The PCC's workforce will ensure that they are aware of how to use social networking sites / tools securely, so as not to compromise their professional role.

7. Monitoring of network and use of ICT facilities

The PCC reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited;
- Bandwidth usage;
- Email accounts;
- Telephone calls;
- User activity / access logs; and
- Any other electronic communications.

Only those authorised by the FBP may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The PCC monitors its ICT use in order to:

- Obtain information related to school business;
- Investigate compliance with PCC policies, procedures and standards;
- Ensure effective PCC and ICT operation;
- Conduct training or quality control exercises;
- Prevent or detect crime; and / or
- Comply with a subject access request, a Freedom of Information Act request, or any other legal obligation.

8. Agreement signature

Please sign below to say that you have read and understood this information.

Name: Signature:

Date: