Stranton PCC: Policy for Use of Information Technology ("IT") Equipment and Services

1. Scope

This policy applies to the use of IT equipment, software applications, network connection and data storage by employees and volunteers who are provided with these by Stranton PCC for use in their work. IT equipment includes desktop and laptop computers, mobile phones, tablet computers, image projectors, printers, network routers and switches and other internet devices.

This policy does not apply strictly to use of private or domestic IT for Church purposes, although clergy, church officers and volunteers who use personal IT for church functions are required to adhere to data protection regulations in holding any work related personal data pertaining to others on their own IT equipment or storage as necessary for performing their roles and responsibilities for the Church – i.e. it must be explicitly consented, adequately secured from unauthorised access, only used in accordance with explicit consent and deleted when no longer needed: Guidance on GDPR is attached.

2. Related policies

- GDPR,
- IT Communications and Social Media
- Disciplinary
- Safeguarding
- Health and Safety (Screen use and posture, manual handling))
- Fire safety

3. Principles

3.1 Safety

Use of IT equipment must be conducted under safe conditions: The Health and Safety (Display Screen Equipment- "DSE") Regulations apply to any workers or volunteers who use DSE daily, for an hour or more at a time, and the PCC's responsibilities include:

- DSE workstation assessment (for postural and eyesight safety) and provision of aids and appliances (such as footrests and adapted pointing devices or screens) where necessary
- reducing risks e.g. taking regular breaks from DSE work, or doing something different
- providing eye tests for DSE workers and volunteers, if requested
- providing training and information for workers and volunteers in correct use of IT equipment.
- IT Equipment and cabling will be PAT tested in accordance with Fire Safety policy
- Manual handling training will include safe lifting and handling of heavy IT equipment

3.2 Security

Employees and Volunteers will be asked to sign a receipt for IT equipment issued to them for personal use (i.e. that they will normally take out of the office). IT equipment is to be kept secure from theft, physical damage, unauthorised access, and malware. Equipment must not be left unattended in cars, or unlocked, or in unattended rooms, and should be password protected, using

“Strong” password techniques, with changes of password at not more than three monthly intervals. When a laptop or computer is switched on in an office or public space and its user leaves it for even a short time, it must be “Screen locked” to prevent unauthorised use.

Users are subject to GDPR requirements for protection of personal identifiable data, and any data breach (unauthorised disclosure or “hacking”) must be reported under the data protection policy.

3.3 Integrity

Only authorised software applications may be used: these include operating systems, web browsers, Office applications, utility software pre-installed by the supplier, antivirus programs, remote meetings software, worship and presentation software, and any other software approved for specific purposes by the PCC appointed administrators. Users will not be granted local administrator rights to install software, the PCC will approve software administrator(s) to review and implement requests for additional software according to specified needs. IT equipment will be configured accordingly.

An Information Asset Register will be kept of the various types of information being stored and who is responsible as “data owner” for each type of data, for legal compliance including retention periods and responsibility for the full deletion of personal data when no longer needed.

Examples of various types of data include

- Contact lists and details for GDPR permission
- Powerpoint presentations
- Video and Audio materials
- Management reports
- Email account folders

Version control will be applied to official documents to enable users to identify current information when needed. Equipment that is internet enabled must be subjected to system and application software update checks at least monthly.

4. IT “Housekeeping”

4.1 Backups

Where applicable, a “system restore disk” will be kept offsite (Church safe) for each item of IT equipment.

Data will be secured in cloud storage using approved software as directed (e.g. Office 365) and a backup schedule and archive arrangements will be agreed with the data owner for each type of data being held. Folder permissions will be managed to prevent unauthorised access from backups.

4.2 Fair personal use

Staff (employees and volunteers) may make limited personal use of IT equipment for the following purposes, at work break or lunch times:

- Access to personal webmail

- Online personal Shopping or Banking Services
- Access to personal online music or radio, but excluding high volume video streaming services
- Pre-installed games
- Online Education or research including short video clips
- Short online personal meetings and social media use.

Under this policy, inappropriate personal use, e.g. for access to or posting of material that is offensive to others or excessive or attracts malware affecting system performance through high volumes of data streaming (e.g. online games) may constitute a disciplinary breach. ***Personal use is not "Private" use and any content including locally saved files and browsing history stored on IT equipment provided will be accessible to the system administrators.***

4.3 IT support

"First line" IT support will be provided by PCC appointed named administrators, who will determine any further repair or remedial action required if the user experiences difficulty in use. Users should report any issues or problems in use of IT to an administrator, unless there is a Safeguarding issue or aspect (e.g. from a suspected data breach by hacking) in which case the Parish Safeguarding Officer must be contacted. Equipment must be handed over for maintenance or upgrade promptly when requested and returned at the end of the period of employment/volunteering.

4.4 Email services

Where the Church provides an official work email account as part of the package of IT equipment and services to an employee or volunteer, that account is to be used for all work related emails sent by that individual, and so far as possible it should be advertised and used for receipt of work related emails. Forwarding by email configuration rules to personal email accounts must not be applied. Download of attachments and email web-links must be subject to sense and virus/malware checks.

4.5 Removable storage

Removable storage devices (Memory sticks, Secure Digital cards, external Hard Disk Devices) are inherently non-secure and must not be used for backup or storage, even when encrypted, as they are easy to lose. If they are used to transfer files to/from third party computers they must be virus checked afterwards. Their use is restricted to:

- Transferring files data in a controlled and lawful manner between IT devices
- Providing visual presentation or worship materials where necessary for public presentation

5. Statement of Policy

In accordance with the stated principles, IT Equipment will be issued and used in a manner that complies with legal and regulatory requirements, ensures the health safety and welfare of users and data subjects, safeguards the reputation of (and investment by) the church, enables effective management, minimises risks and maximises the benefits of IT use.

6. **Review:** This policy will be reviewed initially three months after implementation and thereafter annually.