Policy: IT

This policy relates to the use of any IT devices, either in stand-alone mode or connected to the church network or the internet. It also relates to the security of data when used by St Paul's staff in the course of their employment. For the purposes of this policy, 'device' refers to any IT hardware including PCs, laptops, tablets, smartphones, printers and scanners.

Church IT equipment

Staff and volunteers should note that:

- Any IT equipment provided by St Paul's Church is primarily for the church's work
- The church prohibits the accessing, downloading or distribution of any materials or making any statements or comments that are pornographic, racist, sexist or otherwise discriminatory, illegal or offensive.
- Staff and volunteers are prohibited from sending defamatory, abusive, sexist or racist messages in any form on any media.
- Software may only be installed on church devices with the permission of the incumbent or the IT adviser and must be properly licensed. You must not make additional copies of any licensed software.
- Internet access may only be used as permitted by the church. Other church policies will apply to conduct when using the internet. When using the internet:
  - Do not engage in any activity that might be harmful to systems or devices, or to any information stored on them.
  - Beware of opening email attachments and of clicking on links in emails, on social media sites or on the internet, unless they are verifiably reliable and from known and trusted sources.
  - The internet at St Paul's must never be used for:
    - gambling;
    - viewing or downloading pornographic or obscene material;
    - anything that may damage the interests or reputation of the church;
    - attempting to circumvent or subvert system or network security measures;
    - representing yourself as another person.
  - Remember that websites, newsgroups, forums, chat rooms and social media are public forums where it is inappropriate to reveal confidential information.
- If you leave the church's employment, you should delete all personal files from your devices but not those related to your post and return all IT equipment provided by the church unless some alternative arrangement is agreed. You must delete any church files from all personal devices, including contact details which you have acquired as a result of your employment.

IT Security

In order to satisfy GDPR (General Data Protection Regulation) and Charity Commission advice, any device on which you store any personal, pastoral, safeguarding, personnel or financial information regarding individuals, including both devices purchased by St Paul's and devices owned by staff members and used for work purposes, must comply with the following:

- Your device must be password protected and require password entry after going to screen saver. We recommend that you set your screen saver to activate after a maximum of 15 minutes of inactivity.
- If others use your device, a separate account should be set up for them.
- All devices must have up to date virus protection software.
- Passwords for an account should be different from passwords of any other account and not be easily guessable.
- Where it is an option, use 2 step verification for any church account (or other accounts if used for church business).
- If backing up files to a cloud storage service, files containing personal information must be password protected. External hard drives should not be used.
- You should permanently delete/destroy information as soon as it is out of date/irrelevant, or the period that the information should be kept for has passed. (Contact the Operations Manager if you are unsure how long data should be kept.)
- You should destroy/securely store the hard drive of your device when upgrading/replacing. When replacing your phone, you should do a full factory reset.
- Hard copy information must be stored in a locked filing cabinet.
- In the event of a data breach, including the loss of a device which St Paul's data was stored on, please inform the Operations Manager as soon as possible.

Storage of such data should comply with the St Paul's Kingston Data Protection Policy.

E-Mails

When sending e-mails, via your church email or via ChurchSuite:

- Take care over the language used to reduce the risk of misinterpretation. Re-read messages before sending to ensure that an appropriate tone has been used which balances informality with professionalism. Avoid sending angry e-mails.
- Use blind copies when it is appropriate to preserve confidentiality of email addresses
- Avoid sending confidential or sensitive information by e-mail.
- Do not use your work email address for personal emails.

Staff may access their own personal email during work hours but are asked to keep this to a minimum. Use of the church's e-mail system is not private and may be subject to scrutiny.

Social Media

Staff may use social media in the course of their work and in their own time. Staff are entitled to express their own views and opinions, but should bear in mind that comments posted online are open to being republished in other media and are thus being placed in the public domain, *even if they are initially posted in a private context*. Even posts made in a private capacity may be seen as representative of the church, so staff should be careful about what they post at all times, not only when at work.

When using St Paul's social media accounts:

- Remember you are representing the church, ensure tone and content is always appropriate.
- The audience on social media is wider than the church membership, content should be adjusted appropriately.
- Monitor comments and visitor posts and delete anything inappropriate.
- All communication with individuals is subject to the same safeguarding requirements as in-person contact. If you become aware of a safeguarding issue through social media, you must make our Safeguarding Officer aware immediately.
- See our Communications Policy for more details.

Children and young people

Those working with children and young people should take especial care when using any form of electronic communication, including email, Facebook, Twitter, WhatsApp, etc. Written parental consent for this is essential, and should explain both the form(s) of such communication and how it will be used. The worker's line manager must be made aware when young people are being contacted using electronic communication. It must be for reasons relating to work, not for general socialising, and comply with safeguarding guidance issued by Southwark Diocese.

I agree to abide by this IT Policy

Signature: ____

Name: ____

Date: ____

Written: February 2022
Approved by PCC: March 2022
Reviewed January 2024