Bishop Hannington Memorial Church PCC Policy Statement

Church Computer Use Policy

1. Introduction

Bishop Hannington Memorial Church (hereafter 'the church') requires that BH staff and regular users (see below for occasional users) of its PCs, laptops, tablets and mobile devices, etc (hereafter "computers") and networks agree to abide by the terms of this policy, and sign the user's agreement prior to use. Only those people who have signed the agreement and have been approved by the church operations manager, vicar or churchwardens will normally be permitted to use the church's computers and resources (hereafter 'IT resources'). Priority of use of IT resources must always be given to employees to carry out their duties for which they are employed.

The church requires computer users (hereafter 'users') to abide by standards of appropriate behaviour when accessing the Internet, sending e-mails, using social media and otherwise using computers and networks ("using the IT Resources"). This policy applies to all users. These standards are primarily intended to protect the church's reputation, avoid illegality and ensure that individual rights are not infringed. Extreme cases of inappropriate use could lead to legal proceedings against the church or against individuals.

In order to monitor compliance with this policy the church may monitor all use of the IT resources.

2. Extent of policy

This policy document relates to the use of IT resources owned or operated by the church. This will include IT resources owned by the church whether used on the church premises or in the homes of staff or volunteers, or other computer systems (eg cloud based) set up and managed by the church. It does not extend to computers owned by staff members, church officers, etc. which may be used on church business. Policy relating to the use of personally owned computers on church business will be addressed through other policies such the child protection policy, conditions of employment, volunteer agreements, etc. but all people using personally owned computers on church business, or on the church premises, will be expected to operate within the spirit of this policy.

3. Relevant Legislation

Use of IT resources is subject to the provisions of UK legislation. Users should at all times ensure that their use of IT resources does not contravene any legislation which may be relevant to their work and/or use of IT resources.

4. Security

Users are required to take all reasonable steps to ensure the security of church equipment and data and, in particular,

- Not permit access to IT resources by unauthorised persons (that is people who have not been approved by the church operations manager, vicar or church wardens and signed the user's agreement).

- All church computer user accounts should be protected by password (apart from the Church Member account that only has access to the internet and the printer). Passwords should not be disclosed to any person who has not been authorised to have access to IT resources and the relevant user account by the church wardens or church operations manager. All passwords relating to the church's use of IT resources should be notified to the church operations manager and details kept in the church safe. IT resources should be "password locked" if left unattended.

- Laptops, tablets or other mobile devices should not be left unattended. When stored in the church they should be kept in a locked cupboard.

- Software should only be used in accordance with the terms of the relevant licence agreements for that software.

- Virus protection procedures should be followed at all times - this includes ensuring that any data file to be loaded from CD, disk or other electronic media is virus checked.

- Computer user accounts will be administered by the Church Operations Manager in consultation with the churchwardens.

- Any electronic files with personal or sensitive information (eg on giving) or finance files should be password protected if stored (even temporarily) on any device where guest accounts may be used and where guests could access such files, these passwords to be stored in the church safe.

5. Occasional/Guest Users

Occasional users (visitors, premises users, church members, etc.) may be given access to the "church member account" or access to the wifi at the discretion of the church operations manager, staff members or churchwardens but should not under any circumstances be given details of IT passwords or other security relevant information .

6. Misuse of IT Resources

IT resources may not be used for any illegal or unethical purpose or for a purpose inconsistent with the ethos and values of the church or which might open the church to damage to its reputation or financial loss. Such activities include, but may not necessarily be limited to, the following:

- Viewing, retrieving or downloading pornographic material or any other offensive or objectionable material or knowingly visit sites that contain such materials.

- Sending or posting messages that are abusive, sexist, racist, defamatory, threatening or harassing.

- Use for any unlawful purpose, disclosure of confidential information or trade secrets, defamatory comments, obscenity or harassment

- Disclosing confidential information, defined by the General Data Protection Regulations (GDPR).

- Publicly posting any item on the internet or social media site, on behalf of the church, without permission from the vicar, a church warden or the church operations manager.

- Entering into any contractual commitments by e-mail or over the Internet without prior approval from the church operations manager.

Users who misuse IT resources may face informal or formal disciplinary action, including their right to be a user.

7. Duty of care

Users are required to exercise care in the use of IT resources particularly in relation to incorrect statements of fact made negligently or incorrectly or deliberately which may result in liability on the part of the church to pay damages. Accordingly, users should use all reasonable skill and care in their composition and, where expressions of opinion are set out a suitable disclaimer making clear that opinions expressed are those of the author and not necessarily of the church.

Users should not download any file if they have any doubt as to its source. Users should take care if receiving an attachment from a person they do not know (or someone they do know when they were not expecting it) or if it is of an unusual nature, as many viruses are transmitted in this way.

Discretion should be used when signing up for electronic newsletters or online services that generate automatic e-mail responses.

8. Private use

IT resources are provided for furthering the church's ministry.

Users may, however, make incidental personal (non-business) use of IT resources (for example, internet browsing or email). Incidental use is defined to be of such a low-level the extent of personal use is small compared with ministry use and there is no effect on the performance of the individual in performing their duties.

The church's IT resources may not be used for any commercial purpose.

Adopted by the PCC 22 March 2022 (replacing policy statement adopted on 28 January 2020, 29 January 2019 and 24 January 2017)