High Kirk Presbyterian Church - IT Security Policy

1/ Background. High Kirk is committed to using IT systems in a responsible manner, fully compliant with the requirements of the General Data Protection Regulations (GDPR). IT Security is an important factor in complying with the regulations. This document sets out the churches policies with regard to IT Security, and is relevant to all staff, members, volunteers, and anyone who uses any IT system which contains personal or sensitive information, in connection with High Kirk.

The Congregational Committee is responsible for ensuring compliance with this policy, and delegates certain aspects of its implementation to the Technology Sub-Committee.

2/ Systems. Servers and backup systems shall be located in secure areas, not accessible by the general public, and only accessible to staff and church members who have a specific requirement to enter these areas. Server and computer operating systems shall be maintained with the latest security patches, applied where possible, by automated methods.

Access to the comms room which contains the server is strictly limited to the technical team, the caretaker, and contractors working under the supervision of the caretaker.

Software should only be installed on church owned computers by members of the Technology team.

3/ Administrators and access to data. It is recognised that system administrators will have access to virtually all information held on IT systems. The number of IT full system administrators shall be limited, and shall be approved by Congregational Committee. The principle of "Privilege Based Access" shall be applied, whereby access to any information or system will depend on the user being allocated specific privileges, which limit them to accessing only that which they specifically need.

4/ Network Security. The church network shall be protected from the internet by a firewall, managed by the IT Administrators. All switches, firewalls and other network components shall be protected by secure passwords. Technical measures shall be used to segregate network traffic for administrative systems, technical systems, and publicly available systems. Computers which are joined to the church Active Directory shall be kept in lockable offices. All computers shall have security software installed.

5/ Users. All users of the IT systems, apart from public WiFi, shall have individual usernames and passwords. Users must not share passwords with others under any circumstances. Users must use secure passwords, and where possible, complexity will be imposed by the operating system. Administrators shall have two accounts – one which allows them to access systems as a normal user, and one which is used exclusively for administrative tasks requiring elevated privileges. All High Kirk staff should have @highkirk.org.uk eMail addresses and these should be used for all communications in relation to their work.

6/ Access to shared information. All areas on servers etc. containing personal or sensitive information shall have a designated owner, and others requiring access to such information will require the permission of the owner. "Shared" folders on the server will be access controlled via group membership.

7/ Data on the move. Staff, leaders, and church members should never remove data from church systems on removable media such as memory sticks. Where users have access via remote devices such as tablets or mobile phones, it is essential that these are password or PIN protected.

8/ Cloud Data. Personal/Sensitive data must not be stored on, or transferred via, cloud based systems such as Dropbox, OneDrive, GoogleDrive, iCloud, Amazon Drive, ShareFile, WeTransfer etc.

9/ Omega. Users of Omega shall have a second set of logon credentials, separate from their Windows logon, to provide an additional layer of security.

10/ Voluntary workers / organisation leaders. Volunteers who process church related data on home computers must give assurance that:-

The computer has up to date anti-virus protection installed

The computer is password protected

The computer is used exclusively by the individual in question, or measures have been taken to ensure that others sharing the computer cannot access data relating to High Kirk

Data is not stored exclusively on the personal computer, i.e. it is a working copy of data stored elsewhere

If data is stored on a laptop, it must be encrypted