INFORMATION AND COMMUNICATIONS TECHNOLOGY

ACCEPTABLE USE POLICY

Author	Robert Keenan
Reviewed by	David Malcolm
Authorised by	
Date	19/01/2018
Version	1.1

Contents

Section	Applies To
1 – 15	CSC Staff
1 – 11, 13 – 15	Presbytery Clarks, Deputy Presbytery Clarks
1 – 5.2, 6 – 10, 13 – 15	Auxiliary Ministers, Ministers, Ministers Development Staff, Ordained Local Ministers, Probationers, Retired Ministers, Judicial Proceedings Panel.
1 -12, 14, 15	Guest's, Consultants.

INFORMATION AND COMMUNICATIONS TECHNOLOGY

ACCEPTABLE USE POLICY

1 INTRODUCTION

1.1 Overview

Information is vital to The Church of Scotland and much reliance is placed on IT (Information Technology Dept.) to manage, store and protect this important commodity. The Church recognises that most services now rely heavily on the use of IT equipment and that further increases in use will occur in the future in line with the development of technology.

It also recognises that the rapid growth of electronic communication, particularly in relation to access and exchange of information requires that controls be introduced to ensure the proper use of IT electronic equipment by staff and thereby protect the Church's interests. This Policy seeks to provide appropriate controls to ensure that users utilise IT equipment in a proper and lawful manner.

This policy applies to all those provided with IT access. This includes all Church of Scotland employees, temporary and agency staff, consultants, IT contractors, suppliers and those responsible for maintenance.

2 OBJECTIVES

The objectives of this policy are to

- Protect the Church’s IT and Information assets.
- Establish a controlled framework for providing access to IT and Information assets.
- Identify and ensure compliance with existing Church policies, procedures and legislation.
- Provide direction and guidance regarding IT use.

3 PRINCIPLES

IT must only be used for the Church’s purposes except for authorised personal use outwith working hours.

All users who make use of the Church's IT facilities must be fully informed of the directives of the policy.

All managers and supervisors must ensure that all members of their teams who are likely to make use of these resources are aware of their obligations under the policy.

4 PERMITTED USE

IT is the property of The Church of Scotland and must be used for legitimate Church purposes only. Users are provided with access to assist them in the performance of their duties.

Reasonable authorised personal use of the IT facilities is permitted outwith working hours. All provisions of this policy apply to any personal use.

All users have a responsibility to use the Church’s IT and information resources in a manner that is consistent with the Church's standards of business conduct as detailed in The Church of Scotland Code of Conduct for Employees which can be found on the intranet.

Abuse or careless use of IT or Information assets may result in suspension of access, or disciplinary procedures being initiated and possibly civil and/or criminal liability.

5 RESPONSIBILITES

5.1 Line Managers and Supervisors

All line managers and supervisors have a responsibility to ensure that:

- Their staff members are aware of and comply with all policies, guidelines and practices for IT use.
- Their guests, visitors or consultants are aware and comply with all policies and guidelines and practices for IT use.
- They approve user requests for access and resources.
- Promptly report actual or suspected unauthorised use to the Information Technology Department, or IT Manager.

5.2 Individual Users

Users have a responsibility to:

- Adhere to organisational policies, practices and guidelines for IT use.
- Use IT facilities for properly authorised purposes only.
- Promptly report actual or suspected unauthorised use to their line manager, Information Technology Department or IT Manager.

6 NO EXPECTATION OF PRIVACY

Employees and others are given IT access to assist them in the performance of their duties.

IT, its information resources and all hardware and software is the property of The Church of Scotland and may be used only for Church purposes, with the exception of such personal use as is permitted within the terms of this policy.

Employees should have no expectation of privacy in anything they create, store, send or receive using the Church of Scotland's IT equipment.

The Church of Scotland has the right to monitor and log any and all aspects of its IT including, but not limited to, monitoring Internet sites visited by users, monitoring Email correspondence, phone usage, chat, blog sites, newsgroup postings, and file transfers.

Email transmissions may be monitored, on an individual basis, subject to the Regulation of Investigatory Powers Act and where authorised by a Manager.

IT systems will be audited on an ongoing and regular basis.

The Church of Scotland will routinely archive certain data and Email systems and provide search facilities for Data Protection and Freedom of Information requests to authorised employees.

The discovery of any unauthorised use may result in suspension of access and/ or Church’s disciplinary procedures being initiated.

7 WAIVER OF PRIVACY RIGHTS

The user expressly waives any right of privacy in anything they create, store, send or receive using the Church's IT systems. The user consents to allow authorised Church personnel to access and review all materials created, stored, sent or received by the user through any Church IT equipment, network or Internet connection.

8 DATA AND AUDIT RETENTION

Data created, stored, sent or received, including system audit logs generated using the Church’s IT equipment may be archived or held in backup format. Deleting a file or an Email does not necessarily guarantee its removal from the IT systems, taking away the control from the individual and providing the Church with responsibility for data retention.

*this functionality has not been implemented on our telephone system

9 PROHIBITED ACTIVITIES

Users will not use, nor try to use, an IT username for any of the following purposes:

9.1 Passwords and authentication

- Allow others access to IT facilities through their own login by the sharing of their passwords, except where the IT Manager approves the use of a shared login. Users are responsible for everything that occurs under their username.
- It is specifically forbidden to write down or disclose your password/PIN.
- Suspected or actual password/PIN compromise should be reported immediately to the IT helpdesk.

9.2 Attempting to break through security controls

- Attempting to breach security controls, whether on the Church's IT systems or those of business or service partners. This includes the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means.
- Hindering or disabling monitoring or protective tools.
- Accessing systems or applications (such as Email) which is not intended for them, even if it is not protected by security controls.
- Deliberately accessing or attempt to use, IT or Information resources for which you do not have authorisation.
- Purporting to be anyone other than yourself.

9.3 Viruses

- Intentionally accessing or transmitting computer viruses and similar software.
- Hindering or disabling security software such as Anti-Virus or Firewall software.

9.4 Inappropriate use

- Intentionally accessing or transmitting material which is obscene, sexually explicit, pornographic, racist, defamatory, intended to deceive, harassing, malicious, misrepresentative or which incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise unacceptable.
- Intentionally doing anything which is illegal.
- Personal political lobbying or promoting or maintaining a personal or private business.

- Any activities that could cause congestion and disruption of network and systems such as the playing of games, inappropriate mass Emailing or use of unauthorised software.

9.5 Illegal copying using IT facilities

- Illegally copying material protected under copyright law or making that material available to others for copying.
- Failing to comply with copyright law and applicable licences that may apply to software files, music files, video files, graphics, documents, messages, and other material downloaded or copied.

9.6 Software

- All software must be installed by, or with the agreement of, authorised IT Department personnel, as appropriate. Downloading or installing software (including, freeware, shareware, games and screensavers) without prior agreement and following procedures set down by the IT Department may result in suspension of access and/or disciplinary action.
- Failing to use software in accordance with its license agreements.

9.7 Hardware

- Unless purchased or authorised by the IT Dept. hardware (including portable media devices such as Memory sticks, PDAs CDs, DVDs, MP3 players, *digital cameras and phones) must not be connected to the network. This includes indirect connection e.g. by attaching a device to a PC. The connection of unauthorised hardware without prior agreement may result in suspension of access and/or disciplinary action.

10 CONFIDENTIALITY

- Information handling must be in accordance with relevant legislation e.g. Data Protection Laws.
- Confidential/sensitive data must not be taken off site or loaded onto non-Church of Scotland computers without proper authority and appropriate risk assessment.
- Users must take reasonable steps to safeguard any confidential information in their possession or control.
- Users will not use any confidential information for their own purposes, or for any other purposes other than performing their duties for the Church of Scotland.
- Unless expressly authorised to do so, the user is prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging or entrusted to The Church of Scotland. Unauthorised dissemination of such material will result in the Church's disciplinary procedures being initiated as well as possible civil and criminal penalties.

*The IT Department do not provide digital cameras

11 PERSONAL USE

- Personal use of the computer network is permitted outwith working hours on the basis that it does not interfere with the normal running of the Church’s business, or result in increased costs to the Church, and that availability of service cannot be guaranteed.
- In practical terms this will mean that activities which consume a lot of network capacity (large image, audio or video files, for example) may be restricted, but that access to other internet services will not normally be constrained, provided they are used in line with the other provisions of this Policy.
- Users will not use the Church’s IT equipment and resources in any outside employment.

12 ACCESSING THE INTERNET

To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to the Church's network must do so through the corporate Internet firewall. Bypassing the Church's computer network by accessing the Internet directly by modem or other means without the written consent of the IT Manager is strictly prohibited and will result in suspension of access and/or the Church’s disciplinary procedures being initiated.

12.1 Blocking sites with inappropriate content

- The Church has the right to utilise software that makes it possible to identify and block access to Internet sites containing material deemed inappropriate in the workplace.
- Intentionally accessing or transmitting material which is suggestive, obscene, sexually explicit, pornographic, racist, defamatory, intended to deceive, harassing, malicious, misrepresentative or which incites or depicts violence, or describes techniques for criminal or terrorist acts will be viewed as breach of this policy.

13 EMAIL SECURITY

13.1 Sensitive Information

Use of Email to send confidential/sensitive information is governed by section 10 of this policy (Confidentiality), including the need to obtain proper authorisation to send information, and to risk assess whether Email is an appropriate medium.

Users must not use anonymous mailing services to conceal their identity when mailing through the internet, falsify Emails to make them appear to originate from someone else, or provide false information to any internet service which requests name, Email address or other details.

13.2 Blocking emails with inappropriate content

- The Church has the right to utilise software that makes it possible to identify and block access Emails containing material deemed inappropriate in the workplace.

- Intentionally accessing or transmitting material which is suggestive, obscene, sexually explicit, pornographic, racist, defamatory, intended to deceive, harassing, malicious, misrepresentative or which incites or depicts violence, or describes techniques for criminal or terrorist acts will be viewed as breach of this policy

14 THE CHURCH RESERVES THE RIGHT TO:

Withdraw or restrict users' access to any computer systems and communications services, including Internet services.

Prohibit or restrict access to certain specific newsgroups, web pages and other Internet resources.

Remove or substitute the hardware or software used to access the Internet at any time and for any reason.

15 RESPONSES TO BREACHES OF POLICY:

If a breach of the policy is suspected, authorised IT Dept. personnel may isolate the workstation from the network, seal the system box for security and remove it for forensic investigation by professional consultants.

The Church may respond to violations of the policy in one or more of the following ways:

- Denial or restriction of computer access for a period

- Denial or restriction of computer access permanently

- Disciplinary procedures being initiated which could result in disciplinary action being taken up to and including dismissal.

Provision of information to the police for possible criminal proceedings

REVIEW

This Acceptable Use Policy will be reviewed in the light of future developments in the use of computer technology.