Bishops' Conference of Scotland

The Bishops' Conference of Scotland

Computer Usage Policy

Table of Contents

Document Control

Title	Computer Usage Policy
Prepared by	Donna Maguire
Approved By	Mgr Hugh Bradley
Date of Approval	11/5/18
Version Number	1.3
Review Frequency	Every 5 years
Next Review Date	2023

Status Control

Version	***Date***	***Status***	***Prepared by***	***Reason for Amendment***
1.3	11/5/18	published	DMM	

COMPUTER USAGE POLICY

1 ABOUT THIS POLICY

Our IT and communications systems are intended to promote effective communication and working practices across BCOS agencies /offices. This Policy outlines the standards you must observe when using these systems, the circumstances in which the BCOS may monitor your use, and the action that BCOS may take in respect of breaches of these standards.

1.1

This policy covers all people associated with the BCOS: clergy, officers, consultants, contractors, volunteers, casual workers, agency workers, parishioners, and anyone who has access to our IT and communication systems. In this policy all of these people are referred to as BCOS Personnel.

1.2

Misuse of IT and communications systems can damage the BCOS and our reputation as well as causing harm and distress to any affected individuals. Breach of this policy by employees may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal or removal from post.

1.3

This Policy does not form part of any contract between you and the BCOS and we may amend it at any time.

2 PERSONNEL RESPONSIBLE FOR THE POLICY

2.1

The BCOS trustees have overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to Directors of individual agencies/offices.

2.2

All BCOS Personnel have a specific responsibility to ensure the fair application of this policy and are responsible for supporting colleagues and ensuring its success.

BCOS IT Support will deal with requests for permission or assistance under any provisions of this policy and may specify certain standards of equipment or procedures to ensure security and compatibility. Please consult with BCOS IT Support prior to purchasing.

3 EQUIPMENT SECURITY AND PASSWORDS

3.1

You are responsible for the security of the equipment allocated to, or used, by you and you must not allow it to be used by anyone other than in accordance with this policy.

3.2

You are responsible for the security of any computer device used by you. You should lock your device or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access the BCOS network should NOT be allowed on the system.

3.3

The BCOS IT Support will generally be responsible for making sure that the software on each BCOS device is kept up to date and that data on those devices are regularly backed up. You are responsible for making sure that software is updated. Please follow advice from BCOS IT Support regarding keeping equipment powered on and connected to Internet to enable these updates to take place

3.4

You should use passwords on all IT equipment, particularly items that you take out of the office. BCOS IT Support can set up encryption for those devices which can support it.

3.5

You must keep your passwords confidential and must not use another person's username and password or make available or allow anyone else to log on using your username and password. When you cease to be a member of BCOS personnel, your password will be reset and you must return any equipment, key fobs or cards.

3.6

Passwords or passcodes to devices may be reset, should your line manager need to gain access to the device.

3.7

If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. BCOS IT Support will set up encryption for those devices which can support it. You should also be aware that, when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

3.8

If travelling outside UK borders, particularly to USA or to hostile regimes, please contact BCOS IT Support for advice prior to taking any equipment (whether BCOS-owned or user-owned) abroad. Regulations at various country borders may require disclosure of information, passwords, etc.

4 SYSTEMS AND DATA SECURITY

4.1

You should not delete, destroy, uninstall, bypass or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

4.2

You must not download or install software from external sources without authorisation from your line manager and from BCOS IT Support. This includes software programmes, instant messaging programmes, screensavers, browser add-ins, photos, video clips and music files. Incoming files and data should always be virus-checked before they are downloaded. If in doubt, staff should seek advice from the BCOS IT Support.

4.3

You must not attach any device or equipment to BCOS systems without authorisation from your line manager and from BCOS IT Support. This includes any USB flash drive, MP3 player, tablet, smartphone, wearable or other similar device, whether connected via the USB port, Bluetooth, infra-red connection or in any other way. This includes connecting to a USB port just to charge up the device, as most devices attempt a data connection even if your intention is only to charge up the device.

4.4

You must not access, insert, or connect to BCOS systems any disks, USB drives, SD cards, or other storage media of unknown origin.

4.5

You must not install, copy or otherwise supply software that is licensed to BCOS to others.

4.6

BCOS IT Support systems monitor all emails passing through the BCOS system for viruses, malware and suspicious activity. You should exercise particular caution when opening unsolicited emails from unknown sources or an email that appears suspicious (for example, if it contains a file whose name ends in .exe). Inform IT Support immediately if you suspect your computer may have a virus or if you have opened any suspicious email attachments or clicked on any suspicious links. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

4.7

You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your role.

4.8

You must be particularly vigilant if you use our IT equipment outside your agency/office premises and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

4.9

If you use a smartphone, this must have tracking enabled so it can be traced if lost or stolen. In addition, smartphones should be able to be deactivated remotely, or wiped remotely, if lost or stolen. Smartphones that do not meet required standards for security may not be used for BCOS purposes.

4.10

Laptop or mobile device users should not access public/free wi-fi to handle confidential or sensitive material.

4.11

BCOS Personnel must report any malware attacks – even suspected incidents – to BCOS IT Support as soon as possible.

4.12

BCOS Personnel must not install, or allow to be installed, hardware that has not been approved by your line manager and by BCOS IT Support.

4.13

BCOS Personnel must not remove or tamper with internal hardware components of equipment, or allow those to be removed/tampered with.

5 EMAIL

(See also separate BCOS email usage policy)

5.1

Although email is a vital communication tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

5.2

You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. Anyone who feels that they are being, or have been, harassed or bullied or is offended by material received from a member of BCOS personnel via email should inform their line manager OR the Human Resources Department.

5.3

You should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything that would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain. Remember that Data Protection legislation gives everyone about whom the BCOS holds personal data the right to be to see all that personal data. This means that any comments made about a person in an email may be seen by that person.

5.4

Email messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

5.5

In general, you should not:

- send, forward or read private emails at work which you would not want a third party to read;
- send or forward chain mail, junk mail, cartoons, jokes or gossip;
- contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list;
- sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;
- agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;
- download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear that the owner of such works allows this;
- send messages from another person's email address (unless authorised) or under an assumed name; and/or
- send confidential messages via email or the internet or by other means of external communication which are known not to be secure.

5.6

When sending bulk distribution emails, all addressees should be blind copied (bcc) so that other addressees cannot see who else has been sent the email. If sending regular bulk emails, consider using a bulk email service. Ask BCOS IT Support for advice.

5.7

If you receive an email in error, you should inform the sender. If you have sent an email in error, contact BCOS IT Support immediately.

5.8

Do not use your own personal email account to send or receive emails which relate to your role in the BCOS. Only use the email account we have provided for you.

6 USING THE INTERNET

6.1

Internet access is provided primarily for the purposes of BCOS business. Occasional personal use may be permitted as set out in paragraph 7.

6.2

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 9.1, such a marker could be a source of embarrassment to the visitor and the BCOS, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

6.3

You should not access any web page or download any image, document or other file from the Internet that could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

6.4

Except as authorised in the proper performance of your role, you should not under any circumstances use our systems to participate in any internet chat room, post messages on any Internet message board or set up or log text or information on a blog or wiki, even in your own time.

7 PERSONAL USE OF BCOS SYSTEMS

7.1

The BCOS permits the incidental use of our Internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls, subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. The BCOS may withdraw permission for it at any time or restrict access at its discretion.

7.2

Personal use must meet the following conditions:

- use must be minimal and, if you are an employee, must take place substantially out of normal working hours
- Tag personal emails as “personal” using the inbuilt Sensitivity option within your email’s Properties. (See BCOS Email usage Policy)
- use must not interfere with the work of your agency/office or with the exercise of your role within the agency/office,
- use must not commit the BCOS to any marginal costs; and
- use must comply with this policy (see in particular paragraph 5 and paragraph 6) and our other policies, including our Data Protection Policy and Privacy Policy.

7.3

You should be aware that personal use of our systems may be monitored (see paragraph 8) and, where breaches of this Policy are found, action may be taken under the Disciplinary Procedure (see paragraph 9). We reserve the right to restrict or prevent access to certain telephone numbers or Internet sites if we consider personal use to be excessive.

8 MONITORING

8.1

Our systems enable us to monitor telephone, email, voicemail, Internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

8.2

CCTV systems monitors the exterior of the some of the BCOS agencies/offices 24 hours a day. (A list of these is available from Data Controller.) This data is recorded.

8.3

BCOS reserves the right to retrieve the contents of email messages or to check Internet usage (including pages visited and searches made) as reasonably necessary in the interests of the BCOS, including for the following purposes:

- to monitor whether use of the email system or the Internet is legitimate and in accordance with this Policy
- to find lost messages or to retrieve messages lost due to computer failure
- to assist in the investigation of alleged wrongdoing; and
- to comply with any legal obligation.

8.4

BCOS IT Support may monitor software and data on systems to verify compliance with policies.

9 PROHIBITED USE OF BCOS SYSTEMS

9.1

Misuse or excessive personal use of agency/offices telephone or email systems or inappropriate Internet use is not permitted and will, if you are an employee, be dealt with under our Disciplinary Procedure. Misuse of the Internet can in some circumstances be a criminal offence. In particular, it is not permitted, and if you are an employee it will usually amount to gross misconduct, to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material: (This list is not exhaustive.)

- pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
- offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our parishioners;
- a false and defamatory statement about any person or organisation;
- material which is discriminatory, offensive, derogatory or may cause offence or embarrassment to others;
- confidential information about your agency/office, the work of the BCOS or any member of BCOS personnel or parishioners (except as authorised in the proper performance of your duties);
- any other statement which is likely to create any criminal or civil liability (for you or the BCOS); and/or
- music or video files or other material in breach of copyright.

Any such action will be treated very seriously and if you are an employee is likely to result in summary dismissal.

9.2

If you are an employee, where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or others involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

10 BYOD (BRING YOUR OWN DEVICE)

10.1

The BCOS will allow the use of specific software applications only on company-owned equipment or that which is approved by BCOS IT Support for use as part of BYOD. Only applications needed for BCOS duties and tasks will be installed and supported on these computers. During the support process, BCOS IT Support may require that BCOS Personnel completely reinstall home and personal computer operating systems and application software.

10.2

BCOS Personnel who agree to utilise their devices for BYOD must not “root”, “jailbreak” or otherwise circumvent the security systems of their devices.

10.3

Software purchased/installed/authorised by BCOS must be used only for creating, editing, and processing BCOS-related materials by BCOS Personnel.

10.4

No "pirated" software, or software which has been changed from its original format, such as hacked or otherwise altered (except for that which has been patched by the manufacturer or vendor) is to be used on company systems or those approved for BYOD usage.

10.5

BCOS Personnel utilising their own devices via BYOD should coordinate any installation/update/removal efforts with BCOS IT Support in order to maintain a consistent and well-documented environment.

10.6

If BCOS IT Support determines that a BYOD device no longer meets security standards, the device must no longer be used for BCOS business. The BYOD device will need to be wiped of BCOS data, which may involve inspection by BCOS IT Support.

10.7

General operating system/software/hardware issues with BYOD devices are not the responsibility of BCOS and should be resolved by the vendor or a third-party agency where applicable. However, BCOS data must be wiped from the BYOD device, prior to access by the vendor or third-party. BCOS Personnel are also responsible for ensuring BYOD devices receive regular application and operating system updates.

10.8

BCOS bears no responsibility if the installation or use of any necessary remote access and/or security software causes system lockups, crashes, or complete or partial data loss. BCOS Personnel are solely responsible for backing up their own data on BYOD devices before beginning any BCOS work and before connecting the BYOD devices to BCOS networks or resources.

10.9

If BCOS Personnel believe equipment used to remotely access BCOS resources, systems, and networks might be infected with a virus, spyware infection, or other malware threat or that it might be somehow compromised, they must immediately notify BCOS IT Support of the potential security risk and make the equipment available for analysis and remediation.

10.10

If BCOS Personnel loses or misplaces a BYOD device, they must immediately notify BCOS IT Support of the potential security risk. BCOS IT Support may then remotely wipe the device(s), change passwords, or lock the user's account as needed.

10.11

It is the responsibility of BCOS Personnel to replace lost/stolen BYOD devices.

10.12

From time to time, BCOS IT Support may require to inspect BYOD devices to ensure compliance with this policy.

10.13

You should not discard previously authorised BYOD devices until BCOS IT Support approves the device for disposal.

10.14

Whenever you decommission, prepare to return, or otherwise cease using a personally owned or BCOS-provided device authorised for BCOS use, you should notify BCOS IT Support that the device will no longer be used to connect to BCOS resources, systems, and networks.

10.15

You should not use your own USB thumb drives, SD cards, or other storage media for BCoS purposes.