INFORMATION AND COMMUNICATIONS TECHNOLOGY

BRING YOUR OWN DEVICE POLICY

BYOD

Author	David Malcolm
Reviewed by	David Malcolm
Authorised by	
Date	21/08/2019
Version	1.1

Contents

BYOD Policy

Use of Personally Owned Devices for Church of Scotland Work

1. Purpose

1.1. The purpose of this policy is to ensure that all those who access the Church of Scotland network or Guest Networks, including but not limited to: CSC staff; ministers; MDS staff; and visitors using guest Wi-Fi, including contractors, through their own device(s), such as smart phones, tablet computers, laptops, netbooks and similar equipment (for the purposes of this policy collectively referred to as "Personal Device") to work from home or bring such devices in to work, do so in accordance with the requirements contained in data protection legislation.

1.2. This policy covers anyone who uses a Personal Device to store, access, carry, transmit, receive or use information or data accessible from the Church of Scotland Network Infrastructure maintained by the national office, whether on an occasional or regular basis.

1.3. The purpose of this policy is to reduce risk to the Church of Scotland in individuals using Personal Devices to access data, information and services maintained on the national office's servers. Such risks may come from your Personal Device being lost, stolen, used or exploited in such a way to take advantage of you or the Church of Scotland.

1.4. This policy sets out the minimum requirements employees should adopt to protect data while working from home or when bringing their own Personal Device to work. This policy should be read in conjunction with the Data Protection, Acceptable Use and Social Media policies. Individual departments may specify additional and/or higher requirements as necessary.

1.5. Following the procedures set out below will benefit staff through protection of personal data as well as information assets of the Church of Scotland.

2. General Principles

2.1 Data protection legislation requires all organisations to process personal data (information identifying a living person) in accordance with data protection principles. "Processing" data includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and disposing of it. Organisations must ensure that personal data is protected, by appropriate technical and organisational measures, against unauthorised or unlawful processing or disclosure and against accidental loss, damage or destruction.

2.2 All CSC staff are permitted to use Personal Devices for work related purposes. If you use your own Personal Device for Church of Scotland work, it is important to ensure that it and the information it contains are appropriately protected.

3. Data Sensitivity

3.1 If you access information held within the national office using a Personal Device and your work involves the use of personal data it is likely that at least some of it will find a way on to your Personal Device, for example within your email, or if working on documents away from your office. Given that such information is connected with the Church of Scotland it would be likely to fall under the "Special Categories" of Personal Data, as defined by data protection legislation. Processing such data requires a high level of security.

4. Security obligations for Personal Devices

4.1 If you use a Personal Device to access or use information or data accessible from the Church of Scotland servers maintained by the national office the following provisions apply:

Any type of Personal Device

- Set and use a strong passcode (e.g. pin number or password) to access your Personal Device. Do not share the passcode with anyone.
- Set your Personal Device to lock automatically when it is inactive for more than 5 minutes or if an incorrect passcode is entered after several attempts.
- All devices should be subject to mobile-device management so that if the Personal Device is stolen, upgraded, recycled for money or given to family or friends, the device owner is able to locate the Personal Device remotely and delete the data on demand. The device owner must limit the purpose of the mobile-device management to the detection of the Personal Device and the remote deletion of data.
- Take appropriate physical security measures. Do not leave your Personal Device unattended.
- Keep your software up to date; ensuring that it is genuine software installed under an appropriate agreement between the device owner and relevant manufacturer to prevent any security vulnerabilities.
- Make arrangements to back up your documents.
- Keep master copies of documents on secure storage devices rather than storing documents on Personal Devices.
- The preference is for Personal Devices used to access data on Church of Scotland servers maintained by the national office not to be shared with others. If however other members of your household use your Personal Device, ensure they cannot access Church of Scotland information, for example by using an additional account passcode.
- Organise and regularly review the information on your Personal Device. Delete Church of Scotland information from your Personal Device when no longer needed.

- When you stop using your Personal Device (for example because you have replaced it) or when you leave the Church of Scotland's employment or appointment, or if you stop volunteering for the Church of Scotland, securely delete all Church of Scotland information from your Personal Device.
- Use encryption software on your Personal Device to prevent access even if someone extracts the storage chips or disks and houses them in another Personal Device.[1, 2]
- If data is transferred by email or by other means ensure it is done via an encrypted channel (for example a VPN for individual services).
- **Immediately report any data breaches, including the loss or theft of a Personal Device used for Church of Scotland related activities, to the Law Department by emailing:**

  Lawdept@churchofscotland.org.uk with the subject heading "Data Breach". CSC employees should also report to HR.
- Configure your Personal Device to maximise its security. For example each new technology brings new enhanced security features. Take time to study and discover how to use these and decide which of them are relevant to you. Contact the Church of Scotland IT department in the national offices should you require assistance.
- Whenever possible, use remote access facilities, rather than Personal Devices, to access information on Church of Scotland systems maintained by the national office. Log out and disconnect at the end of each session.
- If you require any technical support with your Personal Devices, you should ensure that the third party providing such support does not have access to personal data for which the Church of Scotland is responsible (for example work emails). Also ensure that no data is transferred from your Personal Device to a third-party device unless there is no other way of rectifying the technical problem. If data is transferred to a third-party device the third party must warrant, and the device owner must ensure, that the information is removed permanently from such third-party devices once the problem has been rectified.
- Anyone who has access to data via Church of Scotland servers maintained by the national offices must delete all personal data obtained from that source when their connection with the national offices ends. In the case of CSC employees that will be when they leave the organisation, at which time all work-related personal data on their Personal Device must be deleted. In other cases that will be at the time at which their appointment or volunteer work with the Church of Scotland comes to an end.

1 *If your Personal Device is an Apple iPhone or iPad, it is encrypted and protection is effective as soon as you set a PIN locking code.*

2 *If your Personal Device is Android, there is an option to turn on whole-Personal Device encryption in its configuration settings. Other devices may or may not be encryptable. We recommend that you include your ability to encrypt as a factor when you are choosing your own devices.*

Mobile phones, smartphones and "tablet" devices

- If the Personal Device is lost or stolen, you must be able to wipe any confidential data on the Personal Device immediately by way of remote "locate and wipe" facility.

- If your Personal Device is second hand, restore it to factory settings before using it for the first time.
- Only download applications ('apps') or other software from reputable sources that are verified and trusted and that will not pose a threat to the security of the information held on the devices.

Laptops, computers and more sophisticated tablet devices

- Use anti-virus software and keep it up to date.

Using wireless networks outside the Church of Scotland

- Control your Personal Device's connections by disabling automatic connection to open, unsecured Wi-Fi networks and make risk-conscious decisions before connecting.
- Assess the security of any open network or Wi-Fi connection noting that you should not use unsecured Wi-Fi networks.
- Disable services such as Bluetooth and wireless if you are not using them.
- CSC employees must not use public cloud-based sharing or public back-up services without prior authorisation from the IT Department.

Deletion of personal data

4.2 You must ensure that if you delete information, it is deleted permanently rather than left in the Personal Device's waste-management system. You may need to use overwriting software to achieve this. However, this is not always practicable because, for example, the information is stored or categorised with other information that is still live. In these circumstances, it is sufficient to put the information "beyond use". This means that you must:

- ensure that you do not use the personal information to make any decision that affects an individual or in a manner that affects an individual in any way;
- not give any other organisation access to the personal data in any way;
- surround the personal data with appropriate technical and organisational security; and commit to the permanent deletion of the information if and when this becomes possible.

4.3 If you use removable media, for example a USB stick, to transfer personal data, you must ensure that the personal data is deleted once the transfer is complete.

Co-operation with subject access requests

Any individual has the right to request copies of personal information of which he/she is the subject (a "subject access request").See the Church of Scotland UCC for more information http://sp-win2k8v.church.cofs/HR/Shared%20Documents/Policies%20and%20Guidance%20Notes/Data%20Protectio n%20Policy%20and%20Guidance/Data%20Protection%20Policy%20UCC.pdf

4.4 . This means that, if an individual submits a subject access request to the Church of Scotland national offices your Personal Device may need to be accessed in order to retrieve data held on it that has been obtained from the Church of Scotland. You must allow the Church of Scotland to access the Personal Device and to carry out a search to find any information about the individual held on the Personal Device.

Monitoring

4.5 As part of its ongoing obligations under data protection legislation, the Church of Scotland national office will monitor data protection compliance in general and compliance with this policy. Please see the Acceptable Use Policy for further detail. This monitoring is in the organisation's legitimate interests, to ensure that the policy is being complied with and to ensure that the organisation is complying with its legal obligations.

5. Consequences of non-compliance

5.1. If an employee is suspected of breaching this policy the organisation will investigate the matter under its disciplinary procedure. If any breaches are established this could result in disciplinary action up to and including dismissal. An employee may also incur personal criminal liability, arising from data protection legislation, for breaching this policy.

5.2. All those accessing data and information via the Church of Scotland network have a legal obligation to ensure the appropriate and safe use of that information. Breaches of that obligation may amount to a breach of the terms of your appointment or contract.

5.3. All those falling under the scope of this policy should be aware of the potential, significant, legal, financial and reputational consequences for the Church of Scotland for failure to keep information sufficiently secure.

6. Helpful information

6.1 If you connect to The Church of Scotland email system using your Personal Device please use the secure and preferred Church of Scotland solution which is the built in email client in Android or IPhone.

If you have difficulty configuring Email on Android and IPhone devices. Log a support call with IT.

Review of procedures and training

The CSC will provide training to all employees on data protection matters on induction and on a regular basis thereafter. If an employee considers that they would benefit from refresher training, they should contact the HR Department.

The IT Department, in conjunction with the HR and Law Department will review and ensure compliance with this policy at regular intervals.