MAMIE MARTIN
SINCE 1993
EDUCATING GIRLS. EMPOWERING MALAWI.

BYOD Policy: Use of Personally Owned Devices for MMF Work

1. Audience and purpose

1.1. This policy is for all staff, trustees and volunteers using personally owned devices such as smart phones, tablet computers, laptops, netbooks and similar equipment to store, access, carry, transmit, receive or use MMF information or data, whether on an occasional or regular basis. The term for such devices is BYOD ("bring your own device").

1.2. The MMF recognises the benefits brought by the use of your own devices for MMF activity and welcomes it. It hugely reduces the cost to the organisation of ensuring that all stakeholders can engage in MMF work most effectively. This policy is about reducing the risk in using BYOD. Such risks may come from your BYOD being lost, stolen, used or exploited in such a way to take advantage of you or the MMF.

1.3. This policy sets out the minimum requirements.

1.4. We believe that following the procedures set out below will bring benefits to all users through protection of your own data as well as that of the MMF.

2. General principle

2.1. If you use your own device for MMF activity, it is important to ensure that it and the information it contains is appropriately protected.

3. Data sensitivity

3.1. If some of your work involves the use of personal data or beneficiaries or donors, and you use a BYOD, it is likely that some of it will find a way on to your device, for example within your email, or if you are working on documents away from your office.

4. Advice for all users in relation to any type of device used for MMF activity

4.1. Set and use a secure method of accessing your device. This might be
   - a passcode (e.g. pin number or password). Whenever possible, use a strong passcode. Do not share the passcode with anyone.
   - fingerprint,
   - face recognition
   - or another secure method of accessing the device.

4.2. Set your device to lock automatically when the device is inactive for more than a few minutes.
4.3. Take appropriate physical security measures. Do not leave your device unattended.
4.4. Keep your software up to date.
4.5. Have a back-up system for your documents in place.
4.6. Keep master copies of documents relating to MMF activity on secure shared online storage systems.
4.7. If other members of your household use your device, ensure they cannot access MMF information, for example, with an additional account passcode.
4.8. Organise and regularly review the information on your device. Delete copies from your device when no longer needed.
4.9. Encrypt the device (to prevent access even if someone extracts the storage chips or disks and houses them in another device) [i] [ii].
4.10. Report any data breaches to the Data Protection Lead (MMF Administrator in Scotland) in accordance with GDPR and our Data Protection Policy.
4.11. Configure your 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. Seek help from your IT support person if necessary.
4.12. When you stop using your device (for example because you have replaced it) and when you leave your role within the MMF, securely delete all (non-published) MMF information from your device, after disconnecting it from any shared online spaces.
4.13. If your device is stolen or otherwise comprised, notify the Administrator as soon as possible – see below for further detail.

5. Mobile phones, smart phones and 'tablet' devices

5.1. Configure your device to enable you to remote-wipe it should it become lost[iii].
5.2. If your device is second hand, restore to factory settings before using it for the first time.
5.3. Only download applications ('apps') or other software from reputable sources.

6. Laptops, computers and more sophisticated tablet devices

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

7. Using wireless networks

7.1 Control your device's connections by disabling automatic

connection to open, unsecured Wi-Fi networks and make risk-conscious decisions before connecting.

7.2 Disable services such as Bluetooth and wireless if you are not using them.

8. Compromised devices

8.1 While it is the user's responsibility to ensure that all devices used for MMF activity are secure, accidents can happen and a device can be compromised by theft, hacking or other event.

8.2 You must report the compromise of any such device to the MMF Administrator as soon as possible. The Administrator shall ensure that compromised data is re-secured as soon as possible.

8.3 In the event of a data breach, the MMF administrator will contact appropriate third parties in line with our Data Protection policy.

9 Consequences of non-compliance

9.1 The loss, theft or misuse of a BYOD is personally distressing. If you use MMF-related personal data, it can also have serious consequences for others, for example beneficiaries, donors, partners, staff, trustees and volunteers about whom information is held. In addition, there may be legal, financial and reputational consequences for the MMF under GDPR.

10 Related MMF policies, procedures and guidance

MMF Data Protection Policy
MMF Privacy Statement

Policy approved by the Board on 29th March 2020

Review Date: March 2022

[i] If your device is an Apple iPhone or iPad, it is encrypted and protection is effective as soon as you set a PIN locking code.

[ii] If your device is Android, there is an option to turn on whole-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.

[iii] If you configure your device for use with Office365, you are able to remote wipe it using a service within the MMF