THURMASTON OLD SCHOOL COMMUNITY CENTRE CIO

Use of Personally Owned Devices for the charity's work

Bring Your Own Device Policy V1.1 17 June 2019

1. Introduction

1.1 This policy is for all office holders, staff, and volunteers, using personally owned devices (eg, phones, tablets, laptops, and desktop computers, etc) to store, access, carry, transmit, receive, or use the charity's information for data. This is commonly referred to as BYOD (Bring Your Own Device).

1.2 The Trustee Board recognises that it relies heavily on volunteers who are prepared to use their own devices to enable the work of the charity to take place. This policy is about reducing the risk in processing data on personal devices. Risks may arise from your device being lost, stolen, used, or exploited in such a way to take advantage of you, or the charity.

1.3 Following this policy is likely to bring benefits to you through protection of your own data as well as that of the charity.

1.4 If you use your own device for the charity's work it is important to ensure that it and the information it contains is appropriately protected.

2. What you need to do

2.1 The extent of the action you need to take will depend on whether you have sensitive data (or special category data under GDPR) or not. Special category data includes information that may well be known to the charity, for instance information about somebody's politics, religion, health. It also includes information about ethnicity and sexual orientation. Bank details and information about criminal convictions are sensitive data although they are not specifically mentioned in the regulation.

2.2 If some of your work involves the use of sensitive / special category data then you need to comply with all of the bullet points below.

2.3 If you only work with data that is not sensitive / special category (eg, contact details, rotas) then you need to comply at least with the bullet points marked with a tick.

2.4 Any type of device

- ✓ Set and use a passcode (eg, PIN number or password) to access your device. Whenever possible, use a strong passcode. Do not share the passcode with anyone.
- ✓ Set your device to lock automatically when it is inactive for more than a few minutes.
- ✓ Be security conscious to ensure your device cannot easily be stolen. Do not leave it unattended or in open view in a locked car.
- ✓ Back up your documents.
- ✓ Keep your software up-to-date.
- ✓ Report any data breaches in accordance with the Data Protection Policy.
- ✓ Exercise caution when opening files attached to emails.
- Ensure other people who may use your device, such as family members, cannot access the charity's information. The easiest way to do this is to password protect documents. Another way is to set up a separate account for each user.
- Periodically organise and review the information on your device. Delete information which is no longer needed.
- When you stop using or dispose of your device and / or when you cease to have a role with the charity, securely delete all of the charity's information from your device.
- Configure your device to maximise its security.

2.5 Mobile phones, smart phones, and tablet devices

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

2.6 Laptops, computers, and advanced tablets

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

2.7 Using third-party wireless networks

- ✓ Be careful about connecting to unsecured wireless networks.
- ✓ Disable services such as blue tooth and wireless if you are not using them.

3. Consequences of non-compliance

3.1 The loss, theft, or misuse of a personal device can be distressing to you. If you use sensitive / special category data, it can also have serious consequences for others. The charity could be subject to investigation by the Information Commissioner's Office and might be fined. You may also have personal responsibility. Please help us to keep everybody's personal data safe.

APPROVED BY THE TRUSTEE BOARD ON 17 JUNE 2019