UNIVERSAL CREDIT ESSENTIALS

Device Policy for Volunteers

Do

- Keep your passwords secure.
- Use biometric features to secure the device if possible.
- Keep your operating system updated.
- Be careful who can see your screen when accessing work systems.
- Report lost or stolen devices.
- Be aware of your responsibility for all costs.

Don't

- Don’t share your device or passwords.
- Don’t make copies of data or take screenshots.
- Don’t access systems without authorisation.
- Don’t save work in unapproved locations or applications.

Scope

This policy applies to all volunteers of the organisation who use a device in their role.

Aims

To ensure UCE systems and data are used appropriately, legally and securely.

To ensure devices are used in a manner which protects confidentiality in accordance with GDPR.

To ensure volunteers clearly understand their responsibilities when using their device.

Security of Devices

Devices must be encrypted and have passcode or biometric security if available with a timeout to lock automatically after 5 minutes of inactivity. Jailbroken or rooted devices are strictly prohibited.

Connectivity via WiFi or mobile data contracts will be the responsibility of the device owner.

Responsibilities

Use of a device that has access to an adviser role should be limited to its owner and must not be shared.

Account logon, passwords and pins must be kept confidential and never shared with others.

Volunteers should be conscious of the setting in which devices are being operated and should ensure data and systems displayed are not visible to others.

Data accessed must not be saved to the device or copied off it.

Screenshots relating to users of our service or other staff must not be taken.

Information relating to users of our service or other staff must not be downloaded or saved on your device.

Staff and advisers must inform their volunteer manager if they leave their role with the organisation.

Staff and advisers must comply with all relevant legislation including not using your device whilst driving.

Devices must be maintained as stated in this document.

Volunteers must immediately inform the organisation immediately if:

- Their password has been breached
- They believe any associated accounts may have been compromised
- Their device gets lost or stolen
- Organisational systems are not working normally

Loss or Damage

The organisation will not accept any liability for loss or damage of personal devices.

Volunteers should inform their Volunteer Manager immediately if they lose their device or have it stolen. We will attempt to restrict access to staff access to our system and any relevant materials.

Costs

Volunteers are responsible for all mobile data or WiFi hotspot costs related to your device usage and should monitor these to ensure they have sufficient allowance.