Company Device Use, Care & Maintenance Policy

1. Purpose

This policy outlines the rules for the use, care, and maintenance of company-owned electronic devices. Its purpose is to ensure devices are used appropriately, protected from damage, and maintained in a manner that supports reliable delivery of training, assessment, and administrative functions.

2. Scope

This policy applies to:

- All staff, instructors, assessors, and volunteers using company-owned devices
- All laptops, tablets, phones, and other electronic equipment issued by the organisation
- All activities conducted on company devices, whether on-site or off-site

3. Definitions

Company Device: Any electronic equipment owned, leased, or provided by the organisation for work purposes.

Personal Use: Any activity not directly related to organisational duties, including personal browsing, social media, entertainment, or personal communications.

Care & Maintenance: Actions taken to protect devices from damage, ensure proper functioning, and maintain security.

4. Policy Statement

Company devices are provided strictly for organisational use. Personal use is not permitted. All staff are responsible for the proper care, security, and maintenance of devices assigned to them. Devices must be used in a professional, secure, and responsible manner at all times.

5. Responsibilities

5.1 All Staff

- Use company devices solely for work-related tasks.
- Protect devices from loss, theft, and damage.
- Report any malfunction, damage, or security concern immediately.
- Ensure devices are fully charged before use in training or assessment settings.
- Follow all cybersecurity and data protection procedures.
- Keep devices clean and stored safely when not in use.

5.2 Management / Course Director

- Ensure staff receive appropriate training on device use and care.
- Maintain an inventory of all company devices.
- Oversee repairs, replacements, and updates.

- Review incidents of misuse or damage and take corrective action where required.

6. Acceptable Use

6.1 Permitted Use

Company devices may be used for:

- Delivering training and assessments
- Completing organisational paperwork
- Accessing approved systems, platforms, and communication channels
- Administrative duties related to the organisation

6.2 Prohibited Use

The following activities are strictly prohibited:

- Personal browsing, social media, messaging, or entertainment
- Downloading unauthorised software or applications
- Storing personal files, photos, or media
- Using devices for any non-work-related purpose
- Bypassing security settings or installing unapproved updates
- Allowing family members, friends, or learners to use the device

7. Care & Maintenance Requirements

7.1 Physical Care

- Devices must be transported in protective cases where provided.
- Food and drinks must be kept away from devices.
- Devices must not be left in vehicles, exposed to extreme temperatures, or placed in unsafe environments.
- Charging cables and accessories must be handled carefully and stored properly.

7.2 Operational Care

- Devices must be kept updated with approved software and security patches.
- Staff must ensure adequate battery charge before courses.
- Only approved cloud storage or organisational systems may be used for saving files.
- Devices must be shut down or locked when unattended.

7.3 Damage or Loss

- Any damage, malfunction, or loss must be reported immediately to management.
- Staff may be required to provide an incident report.
- Repeated negligence may result in disciplinary action.

8. Security & Data Protection

- Devices must be password-protected at all times.
- Staff must not share login details or leave devices unlocked.
- Only secure, approved networks should be used for accessing organisational systems.
- All data must be handled in accordance with GDPR and organisational data protection policies.

9. Return of Devices

When staff leave the organisation or change roles:

- All devices, chargers, and accessories must be returned in good working order.
- All organisational data must remain on the device; personal data must not be stored and therefore does not require removal.
- Devices will be inspected before being reassigned.

10. Policy Review

This policy will be reviewed annually or following any significant incident involving device misuse, damage, or security concerns.

If you want, I can also create: