Device User Agreement Policy

Name of Organisation: Pony Partnerships CIC
Venue/Address for which policy applies: All venues
Date of last review: 1st September 2025
Date of next review: 31st August 2026
Name of author: Danielle Mills

1. Introduction

Mobile devices such as smartphones and tablets are valuable tools for communication and service delivery. However, they also present significant security and safeguarding risks. If appropriate security measures are not applied, mobile devices can be used as a gateway for unauthorised access to Pony Partnerships data and IT systems, potentially leading to data breaches, safeguarding concerns, and reputational damage.

Pony Partnerships CIC is committed to protecting its information assets in line with the UK GDPR, the Data Protection Act 2018, the DBS Code of Practice, and Keeping Children Safe in Education (2024). This policy sets out the requirements for the safe and secure use of mobile devices.

2. Scope

This policy applies to:

- All mobile devices (whether owned by Pony Partnerships CIC or staff/volunteers under a Bring Your Own Device arrangement) that access organisational data, networks, or systems.
- Devices include smartphones, tablets, and similar portable technology.
- Exemptions: Where strict adherence is not possible, a risk assessment must be completed and any exemption authorised in writing by the Clinical Lead (Danielle Mills).

3. Roles and Responsibilities

- Board of Directors: Ensure this policy is reviewed annually and fully implemented.
- Manager/Clinical Lead: Oversee compliance, provide training, and investigate breaches.
- All Staff/Volunteers: Follow this policy, report incidents promptly, and take personal responsibility for safeguarding organisational data.

4. Technical Requirements

- Devices must run a supported, security-patched operating system (Android, iOS, or equivalent). Unsupported or outdated versions must not be used.
- Devices must have encryption enabled at all times.
- Devices must be secured with a strong PIN, password, or biometric authentication. Passwords must comply with Pony Partnerships' password policy and must not duplicate organisational credentials.
- Where available, multi-factor authentication (MFA) must be enabled for access to organisational systems.
- Devices not managed by IT must not connect directly to the internal corporate network.
- Devices must have anti-virus and malware protection installed and active when connected to Pony Partnerships networks.

5. User Requirements

- All lost or stolen devices must be reported immediately to the Clinical Lead.
- Any suspicion of unauthorised access to organisational data must be reported without delay. If this involves safeguarding or personal data, reporting obligations under UK GDPR (72-hour requirement) apply.
- Devices must not be “jailbroken” or “rooted.”
- Only applications from official app stores may be installed. Staff must not download unverified or pirated software.
- All devices and apps must be kept up to date with manufacturer patches.
- Work and personal email accounts must not be merged. Company data must only be sent via the official Pony Partnerships email system.
- Work-related documents must only be accessed, stored, or shared via authorised systems (e.g., Office 365).
- Company data must not be backed up or synchronised to personal accounts or storage.
- Devices must not be connected to corporate workstations for personal content backup.
- Electrical safety of all devices used on-site must be ensured by the user.
- Users are responsible for ensuring virus protection is enabled before connecting to Pony Partnerships wireless networks.

6. Safeguarding and Confidentiality

- Mobile devices may hold or access sensitive information relating to children, young people, staff, or volunteers.
- Staff must handle all information in line with the Safeguarding Policy, Privacy Policy, and UK GDPR.
- Screens should be locked when unattended, and information must never be accessed in public areas where confidentiality could be compromised.

7. Monitoring and Compliance

- The organisation reserves the right to audit compliance with this policy, including spot checks on device security.
- Failure to follow this policy may result in disciplinary action and/or withdrawal of IT access.

8. Review

This policy will be reviewed annually or sooner if legislation, statutory guidance, or cyber security best practice changes.