Pony Partnerships CIC

Cyber Security & Information Security Policy – 2025–2026

Name of Organisation: Pony Partnerships CIC
Venue/Address: All venues
Date of Review: 31 March 2026
Date of Next Review: 31 August 2026
Author: Danielle Mills

1. Introduction

Pony Partnerships CIC is committed to protecting its information systems, devices, records, and data from accidental loss, unauthorised access, misuse, corruption, fraud, and cyber-attack.

This policy applies to all staff, volunteers, contractors, associates, directors, and any other person using Pony Partnerships CIC systems, accounts, devices, networks, or data in the course of their work.

This policy should be read alongside the following Pony Partnerships CIC policies and procedures:

- Data Protection & Privacy Policy
- Device User Agreement Policy
- Remote Learning Policy
- Critical Incident Policy, including the IT Disaster Recovery Plan
- Staff/Volunteer Code of Conduct Policy
- Volunteer & Staff Supervision Policy
- Safeguarding Policies
- Lone Working Policy

2. Policy Aims

This policy aims to:

- protect personal data, confidential records, and business information;
- reduce the likelihood and impact of cyber incidents;
- ensure clear minimum-security standards for devices, accounts, systems, and data handling;
- support legal and regulatory compliance, including UK GDPR and Data Protection Act 2018 requirements;
- support Pony Partnerships CIC in meeting insurer cyber security conditions.

3. Scope

This policy applies to:

- all organisation-owned computers, laptops, tablets, mobile phones, removable media, and network equipment;
- all personal devices used to access Pony Partnerships CIC email, files, systems, or records;

- all cloud systems, email platforms, storage locations, and software used for Pony Partnerships CIC business;
- all users with access to Pony Partnerships CIC information.

4. Roles and Responsibilities

Board of Directors

- The Board of Directors is responsible for ensuring that suitable cyber security arrangements are in place, monitored, and reviewed.

Responsible Lead

The Responsible Lead is responsible for:

- overseeing implementation of this policy;
- authorising access to systems and data where appropriate;
- ensuring backups, recovery arrangements, and security controls are in place;
- ensuring staff training is completed and recorded;
- responding to cyber incidents and data breaches in line with relevant procedures.

Staff, Volunteers, Contractors, and Associates

All users are responsible for:

- following this policy and related procedures;
- protecting devices, passwords, and access credentials;
- reporting suspected phishing, fraud, data loss, malware, or security incidents immediately;
- completing required cyber awareness training;
- only using approved systems and methods for business activity.

5. Device Security Requirements

All devices used to access Pony Partnerships CIC systems or data must meet the following minimum requirements:

- be protected by a password, passcode, or biometric control;
- be configured so that access is limited to the named individual user;
- use supported and up-to-date operating systems and software;
- have anti-virus / anti-malware protection installed where applicable;
- have an active firewall enabled where this is available;
- have device encryption enabled where available;
- lock automatically after a short period of inactivity;
- only be used by authorised persons for authorised business purposes.

No device may be used for Pony Partnerships CIC business if it is jailbroken, rooted, unsupported, or otherwise insecure.

Anti-Virus and Malware Protection

All computer equipment and personal devices used to access Pony Partnerships CIC systems must have effective and up-to-date anti-virus or anti-malware protection in place, where such protection is applicable to the device.

Anti-virus software must:

- be configured to update automatically wherever possible;
- be checked regularly by the user;
- be updated at least monthly as a minimum standard if automatic updating is not available;
- be maintained in active working order at all times.

Users must not disable anti-virus, anti-malware, firewall, or other security software unless explicitly authorised for a legitimate technical reason.

Firewalls

All organisation-owned computer equipment must be protected from unauthorised access by an active firewall.

Where personal devices are used for work purposes, users must ensure the device firewall is enabled where this function is available.

Network equipment, routers, and wireless networks used for Pony Partnerships CIC business must be secured with appropriate settings, passwords, and current firmware.

User Accounts, Passwords and Access Control

Access to Pony Partnerships CIC systems and devices must be authenticated using individual user accounts and passwords or equivalent secure credentials.

The following rules apply:

- each user must have their own login credentials;
- shared accounts must not be used unless unavoidable and expressly authorised;
- default passwords and access codes must be changed promptly before devices or systems are put into use;
- passwords must be kept confidential and must not be written down in an insecure manner or shared with others;
- users must not reuse the same password across critical business systems where avoidable;
- accounts must be removed or disabled when a person leaves or no longer requires access;
- access rights must be limited to what is necessary for the person's role.

Multi-factor authentication should be enabled wherever available, particularly for email, cloud storage, finance systems, and administrator accounts.

Security Updates and Patching

Updates to firewalls, firmware, operating systems, applications, software, and security tools must be installed promptly.

Where an update addresses a vulnerability described by the provider as **critical**, **important**, or **high**, or where it has a **CVSS v3 score of 7.0 or above**, the update must be applied within **14 days of release**, unless:

- there is a documented technical reason why immediate application is not possible, and
- alternative mitigating controls are put in place, and
- the delay and rationale are recorded and authorised by the Responsible Lead.
-

Routine security and software updates not falling within the above category must still be applied within a reasonable timeframe.

Data Storage, Backup and Recovery

Pony Partnerships CIC will ensure that essential business data is backed up regularly and that backups are capable of supporting recovery in the event of accidental loss, corruption, device failure, or cyber incident. The following minimum standards apply:

- business-critical data must be backed up at least weekly;
- where automated daily backup is available, this should be used;
- backups must be stored securely and separately from the live working environment;
- backup integrity must be checked and validated on a regular basis;
- restoration testing must take place periodically;
- records of backup checks and recovery tests should be maintained.

Staff must only store business information in approved locations. Personal or sensitive business data must not be stored in unapproved locations or solely on local devices unless unavoidable and appropriately secured.

6. Secure Disposal of Data and Equipment

Personal data and other sensitive business data must be disposed of securely when no longer required and in accordance with applicable retention requirements.

This includes:

- confidential paper waste being shredded or disposed of using secure confidential waste arrangements;
- digital records being deleted securely from systems, devices, and storage media where appropriate;
- devices being wiped, reset, or destroyed securely before disposal, recycling, transfer, or reuse;
- removable media being destroyed or securely erased where needed.

No person may dispose of records or equipment containing personal or confidential information through general waste or informal methods.

7. Email Security, Phishing and Fraud Prevention

Users must exercise caution with all emails, messages, attachments, links, and requests for information or payment.

Staff, volunteers, contractors, and directors must:

- be alert to phishing, spoofed email addresses, fake invoices, urgent payment requests, and impersonation attempts;
- verify unusual or unexpected instructions using a trusted secondary method;
- never disclose passwords or authentication codes in response to an email, message, or phone call
- report suspicious communications immediately;
- avoid downloading attachments or clicking links unless satisfied that they are legitimate.

8. Social Engineering Fraud Training

Pony Partnerships CIC will provide training to staff, directors, and relevant volunteers on cyber security risks, including social engineering fraud, phishing, payment diversion fraud, password security, and data handling.

This training will be:

- completed as part of induction where relevant;
- refreshed at least annually;
- recorded centrally by Pony Partnerships CIC.

Additional updates or briefings may be issued when risks change or when incidents indicate a need for further awareness.

9. Payment Card Industry Compliance

Where Pony Partnerships CIC processes payment card data directly, it will ensure that appropriate Payment Card Industry Data Security Standard requirements are met.

Where card payments are handled entirely through an external provider, Pony Partnerships CIC will use reputable providers and will not retain card details except where expressly permitted and securely managed.

10. Incident Reporting

Any actual or suspected cyber security incident must be reported immediately to the Responsible Lead.

This includes:

- lost or stolen devices;
- malware or ransomware alerts;
- phishing emails clicked or responded to;
- unauthorised access or attempted access;
- disclosure of passwords or security codes;
- misdirected personal data;
- suspicious payment requests;
- data loss, corruption, or service outage.

Incidents will be managed in line with the Critical Incident Policy, IT Disaster Recovery Plan, Privacy Policy, and any data breach reporting obligations.

11. Monitoring and Review

Compliance with this policy may be monitored through supervision, spot checks, training records, device reviews, and incident follow-up.

Breaches of this policy may be treated as a disciplinary matter and may result in removal of system access, contract action, or referral under safeguarding, professional, or legal procedures where appropriate.

This policy will be reviewed annually, or sooner if there is:

- a significant cyber incident;
- a material change in systems or working practices;
- updated legal, regulatory, or insurer requirements.