Pony Partnerships CIC

Cyber Security and Information Security Policy 2026-2027

Name of Organisation: Pony Partnerships CIC
Venue/Address: All venues
Date of Review: 1 September 2026
Date of Next Review: 31 August 2027
Author: Danielle Mills

1. Policy Statement

Pony Partnerships CIC is committed to protecting the confidentiality, integrity and availability of its information, systems, accounts, and devices.

Cyber and information security support:

- safeguarding;
- privacy;
- safe service delivery;
- business continuity;
- organisational resilience.

Everyone working for or on behalf of Pony Partnerships has a responsibility to protect information from unauthorised access, loss, misuse, damage, fraud, and accidental disclosure.

2. Purpose

This policy sets out how Pony Partnerships will:

- protect organisational information and systems;
- manage access to accounts and records;
- support secure use of devices and remote working;
- reduce the risk of phishing, fraud and cyberattack;
- respond to cyber incidents and data breaches;
- protect safeguarding, medical, allergy and other sensitive information;
- maintain essential services following disruption.

Detailed practical requirements are contained in our Standard Operating Procedures.

3. Scope

This policy applies to:

- directors;
- employees;
- associates;

- volunteers;
- students and trainees;
- contractors and authorised third parties with access to systems or information.

It covers:

- computers, laptops, mobile phones, and tablets;
- personal devices authorised for work use;
- email and user accounts;
- Office 365, SharePoint, Teams, and other approved systems;
- websites and online platforms;
- paper and digital records;
- cloud storage;
- remote access and remote working;
- commissioner systems accessed by Pony Partnerships staff.

4. Legal and Regulatory Context

This policy has been developed with regard to relevant UK data protection, cyber security, and information security requirements, including:

- UK GDPR;
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Computer Misuse Act 1990;
- recognised guidance from the National Cyber Security Centre.

Pony Partnerships will use reasonable and proportionate security measures, taking account of the sensitivity of the information, the systems used and the risks to individuals and the organisation.

5. Responsibilities

- Board of Directors: responsible for ensuring that proportionate cyber and information-security arrangements are in place and reviewed.
- CEO/Manager: responsible for:
    - implementing this policy;
    - approving systems and access arrangements;
    - coordinating the response to significant cyber incidents;
    - ensuring data breaches are assessed;
    - arranging appropriate technical support;
    - overseeing notification to affected people, commissioners, insurers, or authorities where required;
    - ensuring learning and corrective actions are completed.
- DSL and DDSL: must be informed where a cyber incident:
    - places a child, young person, or adult at risk;
    - involves safeguarding information;
    - involves harmful or criminal online behaviour;
    - may indicate grooming, exploitation, or cyber-dependent offending.
- Staff, Associates, Volunteers and Other Users: must:
    - follow this policy and SOP 7;
    - use only approved systems;
    - protect accounts and devices;
    - access information only where required for their role;
    - report concerns immediately;

- preserve evidence;
- work within their competence and authority.

6. Approved Systems and Access

Work records must be created, stored, and shared through approved organisational or commissioner systems.

Approved Pony Partnerships systems may include:

- Office 365;
- SharePoint;
- Teams;
- Google Meet:
- approved organisational email;
- other systems expressly authorised by the CEO/Manager.

Access must be:

- limited to what the person needs for their role;
- protected by individual account credentials;
- reviewed when duties change;
- removed when access is no longer required.

Users must not:

- share accounts or passwords;
- access records without a work-related reason;
- use personal email or storage accounts for Pony Partnerships information;
- transfer records to unauthorised systems;
- attempt to bypass security controls.

Commissioner systems must be used only for the agreed purpose and must be logged out or secured after use.

7. Passwords and Authentication

Users must:

- use strong, unique passwords or passphrases;
- keep passwords confidential;
- not reuse organisational passwords on personal accounts;
- use multi-factor authentication where available or required;
- change passwords immediately where compromise is suspected;
- securely lock devices when unattended.

Passwords must not be:

- shared by email, text, or messaging;
- displayed openly;
- stored in an unsecured document or location.

Suspected password compromise must be reported immediately.

8. Devices and Personal Device Use

Devices used for Pony Partnerships work must:

- be protected by a password, PIN, or biometric security;
- use a supported operating system;
- receive appropriate security and software updates;
- be protected from unauthorised access;
- be stored securely when not in use;
- be locked when left unattended.

A BYOD Declaration must be completed before a personal device is used to access organisational systems.

Participant and organisational records must not normally be stored directly on personal devices.

Where temporary downloading is necessary for an authorised work purpose, the information must:

- be protected;
- remain within approved applications or storage;
- be removed securely as soon as it is no longer needed.

Lost, stolen or compromised devices must be reported immediately.

Personal accounts must not be used for participant communication or work records unless an exceptional arrangement has been formally authorised.

9. Email, Phishing, and Fraud

Users must remain alert to:

- phishing emails;
- suspicious links or attachments;
- impersonation attempts;
- fake invoices or payment requests;
- requests for passwords or confidential information;
- unexpected account-reset messages;
- suspicious telephone calls or messages.

Before responding to an unusual request, users must:

- check the sender carefully;
- avoid opening unexpected attachments;
- verify significant requests using a separate and trusted contact method;
- report suspicious activity.

Financial or bank-detail changes must be independently verified through the approved payment-verification process.

Confidential information must only be sent where:

- sharing is authorised;
- the recipient has been checked;
- the method is appropriate and secure.

10. Information Handling and Remote Working

Information must be:

- accessed only where required;
- stored in approved locations;
- shared only with authorised people;
- protected from accidental disclosure;
- disposed of securely when no longer required.

Particular care must be taken with:

- safeguarding records;
- medical and allergy information;
- clinical and healthcare plans;
- emergency medication information;
- contact details;
- commissioned learner records;
- staff and recruitment information.

Paper records must be stored securely and must not be left visible or unattended in public areas.

During remote or flexible working, users must:

- use secure internet connections where reasonably practicable;
- prevent others from viewing information;
- avoid confidential conversations in public places;
- secure papers and devices;
- follow the same access and confidentiality requirements that apply on site.

11. Cyber-Related Safeguarding Concerns

Cyber activity may also create a safeguarding concern.

This may include:

- unauthorised access or hacking;
- malware creation or use;
- denial-of-service activity;
- online exploitation;
- coercion or threats;
- access to harmful or illegal material;
- misuse of participant information;
- behaviour indicating possible involvement in cyber-dependent crime.

Where a child or young person may be at risk, the matter must be reported to the DSL or DDSL.

Staff must not investigate the child's conduct themselves or access devices beyond their role or authority.

The DSL may seek advice or refer to appropriate safeguarding or diversionary support, including Cyber Choices where relevant.

12. Reporting and Responding to Incidents

A suspected cyber or information-security incident must be reported immediately to the CEO/Manager or designated lead.

Examples include:

- phishing;
- malware or ransomware;
- unauthorised access;
- compromised passwords;
- suspicious account activity;
- lost or stolen devices;
- accidental disclosure;
- information sent to the wrong person;
- loss of access to essential systems;
- unauthorised alteration or deletion of records.

The person discovering the incident must:

1. stop further action where this can be done safely;
2. report the matter immediately;
3. preserve relevant emails, messages, screenshots, and other evidence;
4. not delete information or attempt to conceal the incident;
5. not undertake technical action beyond their competence;
6. follow instructions from the CEO/Manager or authorised technical support.

The organisational response may include:

- restricting or suspending access;
- changing passwords;
- securing accounts or devices;
- recalling or containing information;
- identifying information and people affected;
- considering safeguarding risk;
- restoring systems;
- informing commissioners or affected individuals;
- obtaining specialist advice;
- recording and reviewing the incident.

13. Data Breaches and Records

Not every cyber incident involves personal information.

Where personal information may have been lost, disclosed, changed, accessed, or made unavailable without authority, the incident must also be assessed as a possible personal-data breach.

Pony Partnerships will consider:

- what information is affected;
- whose information is involved;
- whether safeguarding or safety is affected;
- the likelihood and seriousness of harm;
- whether affected people should be informed;
- whether notification to the Information Commissioner's Office is required.

The relevant record must be completed:

- Data Breach Record for an actual or suspected personal-data breach;
- Device Loss/Theft Record for a lost or stolen device;
- Cyber Security Incident Record for phishing, malware, compromised accounts or other cyber events.

More than one record may be required where an incident falls into several categories.

14. Business Continuity and Recovery

Pony Partnerships will maintain proportionate arrangements to protect and restore essential information and systems.

Following significant disruption, priority will be given to:

- safeguarding communication;
- access to emergency and medical information;
- communication with participants, families, and commissioners;
- protection of records;
- restoration of approved systems;
- safe continuation or temporary suspension of services.

Systems must only be restored or reconnected when it is considered safe to do so.

A significant cyber incident may also be managed under the Critical Incident and Business Continuity

15. Training and Monitoring

Users will receive information, instruction, and training appropriate to their role.

This may include:

- password and account security;
- phishing and social engineering;
- device security;
- secure information handling;
- safeguarding, medical and allergy information;
- data-breach reporting;
- secure remote working;
- fraud awareness.

Pony Partnerships will review:

- reported incidents;
- recurring concerns;
- user access;
- training needs;
- vulnerabilities;
- the effectiveness of corrective actions.

Learning from incidents and reviews will be used to improve security and resilience.

16. Review

This policy will be reviewed annually, or sooner where:

- legislation or recognised guidance changes;
- a significant cyber threat or incident occurs;
- systems or suppliers change;
- business-continuity arrangements identify a weakness;
- safeguarding or data-protection learning requires a change;
- the Board requests a review.