PWL PATHWAYS LDN
Employment, Skills & Training

Information Security Policy

Version 6.0

Contents

Version Control

Version	Reviewer Name	Date	Next Review	Comments
1.0	Rena Panesar	Dec 2020	Dec 2021	First Policy.
2.0	Rena Panesar	Dec 2021	Dec 2022	Updated.
3.0	Rena Panesar	Dec 2022	Dec 2023	Updated.
4.0	Rena Panesar	Dec 2023	Dec 2024	Updated.
5.0	Paul Tumwine	Dec 2024	Dec 2025	Updated.
6.0	Policy Pros	Oct 2025	Oct 2026	Retemplated and updated.

Introduction and Purpose

This Information Security document aims to provide a structured approach to managing information security risks within our organisation.

The approaches outlined include protecting the integrity of such information, including the devices that store, process, and transmit sensitive data (for example, workstations, laptops and mobile devices), by minimising unauthorised access to Pathways LDN data and our hardware.

If you have any questions or comments about the content of this policy or if you need further information, you should contact our Directors.

Who and what this policy applies to

This policy applies to all individuals working for or on behalf of Pathways LDN.

Responsibilities

The Directors are responsible for ensuring that data controlled and processed by or on behalf of Pathways LDN is protected and that IT security is maintained.

Staff must:

- Agree to comply with the policies and procedures related to IT security contained in this document.
- Agree to comply with any other related policies; for example, our Data Protection and Confidentiality policies.
- Acknowledge that violations of Pathways LDN policies and procedures may result in disciplinary action.

Access Controls

Principles

Pathways LDN follows these principles when determining staff access:

- Least Privilege: Users will only be granted the minimum level of access required to perform their duties.
- Role-Based Access: Access rights will be aligned to job roles and responsibilities.
- Need-to-Know: Sensitive or confidential data will only be accessible to those with a legitimate business requirement.

Access controls are determined by our Directors, who will be the 'superusers'.

Depending on need, staff may be granted limited access to the following:

- Google Drive/other Google software
- Microsoft Office software

When granting access, each user will be given a unique user account/login.

Similarly, learners will be provided with unique user accounts/logins so that their use of our devices and systems can be monitored.

Onboarding/Offboarding

When leaving Pathways LDN's employment and/or where access is no longer required, the individual's access rights are removed.

Monitoring and Auditing

System access logs will be maintained and may be monitored to look for suspicious or unauthorised activity.

Acceptable Use

When using Pathways LDN devices, software and systems, individuals must not:

- Access systems and services using another user's credentials.
- Use our email or other systems, including hardware, for bullying, harassment, or abuse.
- Access, download, send or receive any data (including images) that Pathways LDN considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material. This includes internal communications and channels such as live chat platforms.
- Use email or any other software for distributing spam.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Purposefully install any virus, Trojan, keylogger or other harmful software onto Pathways LDN devices.
- Open attachments that they suspect contain viruses or malware, or ignore generated messages warning of the same.
- Remove or disable Antivirus or other security software.
- Use Pathways LDN devices to participate in DDOS attacks or any other illegal activity related to overloading networks or other cybercrimes.

Individuals must seek authorisation to perform the following actions, whether using Pathways LDN networks or outside of the workplace:

- Place any information on the Internet related to Pathways LDN, alter any information about the organisation or express any opinion about Pathways LDN.
- Send unprotected sensitive or confidential information externally.
- Forward Pathways LDN's email to personal email accounts without prior authorisation.
- Make official commitments through the Internet or email on behalf of Pathways LDN.

Hardware

Hardware Scope

Our current hardware is limited to:

- 7 x Windows Laptops for staff
- 7 x Windows Laptops for learners
- 3 x Apple iPhones

All Company devices benefit from the built-in security controls of operating systems like iOS and Windows.

Access to Hardware

- Devices allocated to staff must only be used for legitimate business purposes. Sharing login credentials or allowing others (including family or friends) to use company hardware is strictly prohibited.
- When learner devices are provided, these must only be used for learning and again, sharing login credentials or allowing others (including family or friends) to use them is strictly prohibited.
- Any suspected tampering or unauthorised access must be reported immediately to the Directors.

Protection from Malware and Unauthorised Access

- Only the Directors and third parties authorised by the Directors may install or configure software on company devices. Staff and learners must not download, install, or run unauthorised software.
- Approved antivirus/endpoint protection software will be managed by our Directors, and will remain active and up to date on all devices.
- Operating system and application updates will be applied promptly to the Directors to reduce security vulnerabilities.

External Media and Storage

- The use of external media or storage devices (e.g., USB drives, external hard drives, memory cards) is not permitted.
- Exceptions require written authorisation from the Directors and must follow strict security controls.

Physical Protection

- Due care and attention should be paid when working at home or remotely.
- Devices should not be left unattended when in public places or stored in vulnerable positions. They should always be securely stored.
- When working from home, users should still lock devices if unattended for a short period and shut them down when not in use for long periods.
- Devices should not be shared with or accessible to other members of the household or other parties.
- A clear desk policy should still apply when away from an office location.
- When accessing personal data, users should be aware that others may be able to see the device screen.

Returning Hardware

- All hardware must be returned to us by staff:
    - When employment ends; or
    - When the staff member is on extended leave (e.g., maternity/paternity leave, long-term sickness, or career breaks).
- All hardware must be returned to us by learners:
    - At the end of the session; or
    - When agreed upon with a Director.
- Failure to return hardware may result in deductions from final pay or legal action to recover the property.

Hardware Disposal and Reissuing

- All company devices that are no longer required or are beyond repair will be securely decommissioned (which will be recorded on the asset register), and all data will be securely erased using industry-approved methods.
- Physical destruction (e.g., shredding or degaussing hard drives) may be used where secure erasure cannot be guaranteed.
- Devices must only be disposed of through approved IT asset disposal providers, ensuring compliance with the Data Protection Act 2018 and UK GDPR.
- Certificates of destruction/disposal will be retained for audit purposes.
- Any device being reissued to another staff member or learner will first be securely wiped of all existing data, applications, and configurations.
- The reallocation will be recorded.

Bring Your Own Device (BYOD)

Pathways LDN acknowledges that staff will sometimes use personal mobile devices (BYOD) for work purposes, such as accessing emails or utilising essential applications. However, this introduces specific security risks that must be managed. Staff using a personal device for work must agree to the following conditions:

- The device must be protected by a strong password or biometric authentication and must have up-to-date operating system security patches installed.
- Staff must take all reasonable steps to ensure that confidential company or learner data accessed on the personal device is not stored directly on the device's main memory or shared with non-work applications.
- Loss or theft of a personal device used for work must be reported immediately (as per the procedure outlined further down in this policy) so that remote wiping procedures can be initiated if company data is deemed to be at risk.
- The use of personal devices for work remains subject to all provisions of this IT and Information Security Policy and the Data Protection Policy.

Password Controls

Password Guidelines

As highly effective means of preventing unauthorised access:

- 2FA Two-factor authentication **must** be used where available. Users must **not** disable or bypass 2FA under any circumstances, and any issues with authentication should be reported immediately to the Directors.
- Biometric security access controls (fingerprint or facial recognition) **must** be used where available.

Unless otherwise specified, passwords must have at least twelve (12) characters and must contain at least:

- One upper-case alphabetic character (A-Z).
- One lower-case alphabetic character (a-z).
- One numeric character (0-9).
- One special character (! ? >).

It is best practice to use a passphrase, which is a long, unique, and hard-to-guess sequence of random words and numbers.

- A good example: *B!ueGardenHorse&River*

Never use easy-to-guess passwords such as:

- *Common words/sequences - Password1234*
- *Personal information - john1985 (name + year of birth)*
- *Keyboard patterns – qwerty789*

In the case of mobile devices and tablets, never use easy-to-guess or repetitive numbers such as '111111' or '123456'.

Password Protection Standards

The following are required for all devices and software:

- Change passwords at least every 30 days as prompted and immediately upon suspicion of compromise or if known disclosure was made to another person.
- Never write passwords down in plain sight; if passwords must be written down, ensure they are stored securely and only accessible to the user. For example, use a secure system such as 'LastPass'.
- Never share passwords with others or ask others for their passwords.
- Avoid the reuse of passwords for different devices/systems/software/applications.

Data Storage and Transmission

Local Storage

Users should not download personal or sensitive data onto their devices – all such data should be stored in our secure cloud-based software solutions.

Data In Transit and At Rest

All stored data is encrypted, both at rest and in transit.

- HTTPS is used by default when using browser-based applications.
- All email traffic uses standard TLS encryption.
- BitLocker encryption is enabled on all Windows devices (via Microsoft Defender).

Data Back-Ups

Business-critical back-ups are managed using cloud-based systems.

Retention Periods

Users should be aware of the retention periods outlined in our policies and perform regular audits on stored data and its relevance.

Secure Transmission

Data transmission must only be conducted using secure methods when handling personal, sensitive, or otherwise confidential information.

Examples of secure and non-secure transmission methods include:

Secure	Non-Secure
Sending the file as an attachment using Microsoft Outlook/Office 365.	Using Apple Messages (iMessage) or WhatsApp for sharing sensitive data.
Uploading and sharing files via SharePoint or OneDrive.	Using an older, non-compliant, or free cloud service (like an unencrypted personal Google Drive or Dropbox) to share documents.
Using approved company online meeting platforms like Microsoft Teams.	Using unapproved online meeting platforms that only use HTTP (not HTTPS).

Best Practice Advice Examples:

- Before sending, verify the Recipient: Always double-check the email addresses, postal addresses, or phone numbers before transmitting sensitive data. If you are unsure of the address or the person receiving it, telephone the recipient to verbally confirm the details.
- Encrypt sensitive attachments: When sending attachments containing highly sensitive data (like medical records, criminal records, bank details, or internal audit reports), password-protect the document itself (e.g., using a protected PDF or Word file). Send the password via a separate, secure channel, such as a phone call or a text message.
- Faxing: If you must fax personal or sensitive data (which is not recommended but may be requested by certain organisations), ensure you use secure fax protocols. Always telephone the receiver before and after sending to verify the machine is monitored and to confirm receipt.
- Safeguarding communications: When communicating with safeguarding teams or external agencies, always use their secure online reporting forms or our secure company email system. Always make sensitive calls from company phones or official communication lines.

If you are ever in doubt about the security of a transmission method, you must ask the Directors for guidance before sending the data.

Wi-Fi

Office/Centre Wi-Fi Security

Network Security

- All office/centre Wi-Fi networks are protected by strong encryption.
- Wi-Fi passwords are complex, unique, and changed regularly, particularly if there is evidence of compromise.
- Filters are in place to block malicious websites, inappropriate content, and known security threats.

Access Control

- Only authorised staff may connect to the internal office Wi-Fi.
- Guest (learner and visitor) access may be provided with time-limited credentials where appropriate.

Monitoring and Maintenance

- Logs will be maintained for security monitoring and reviewed periodically. These logs will assist us in our safeguarding duties where learners access our devices and Wi-Fi.
- Firmware and software updates for Wi-Fi equipment are applied promptly to protect against vulnerabilities.

Staff Responsibilities

- Staff and learners must not share Wi-Fi credentials with unauthorised individuals.
- Any suspected unauthorised access or network issues must be reported immediately to the IT Team.

Use of Public Wi-Fi

- Wherever possible, staff should avoid using public Wi-Fi for business purposes, particularly when accessing personal or sensitive data or otherwise confidential information.
- Wherever possible, mobile data (4G/5G) should be used as a safer alternative if a secure office or home connection is not available.

Safe Usage

The following will help users to prevent data breaches and should be followed:

- Users must always lock their computer, phone, or tablet when stepping away from their device, even for a short period.
- Users should always log out of software applications and systems when they have finished using the application and before they shut their device down.
- Users must be careful when downloading files or clicking on links. Be suspicious of links and other forms of data sent in an email or text message which seem unusual, and avoid downloading software, plugins, or files from unverified sources.
- In public spaces, eavesdropping should be considered before making sensitive calls.
- Users must not use open/unsecured Wi-Fi locations or hotspots when accessing information or systems.

Lost or Stolen Devices

If a Company device is lost or stolen, it must immediately be reported to Rena Panesar, the Director, in person or at rena@pathwaysldnltd.com (or Paul Tumwine on paul@pathwaysldnltd.com in their absence), who will arrange for the device to be remotely wiped or disabled. All relevant software/systems passwords will also be changed.

If any personal device that is used to access Company software is lost or stolen, this must also be reported so that the relevant software/systems passwords can be changed.

Where appropriate, the device owner must also make a Police report in order to obtain a crime reference number.

Data Breach Procedure

- A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed in connection with the provision of a public electronic communications service.
- This means there will be a personal data breach whenever any personal data is accidentally lost, corrupted, or disclosed or if someone accesses it or passes it on without proper authorisation.
- If you think there has been a breach, you must immediately inform Rena Panesar, the Director, in person or at rena@pathwaysldnltd.com (or Paul Tumwine on paul@pathwaysldnltd.com in their absence).
- The breach will be logged, and the risk assessed.
- Swift action will then be taken. This may include, but is not limited to, disconnecting devices from the internet, changing passwords to software and systems, remotely disabling or wiping devices.
- Following containment, the Directors will work to prevent recurrence.
- Depending on the level of risk, we may be required to report it to the ICO within 72 hours.

Non-Compliance

Failure to comply with this Information Security Policy, or any associated policies such as Data Protection and Confidentiality, will be treated seriously. All individuals working for or on behalf of Pathways LDN are expected to understand and adhere to the controls and responsibilities outlined within this document.

Non-compliance may include, but is not limited to:

- Sharing login credentials or allowing unauthorised access to Pathways LDN devices or systems.
- Unauthorised use of company devices or systems.
- Failing to report security incidents, data breaches, or suspected unauthorised access.
- Neglecting to follow required password, access, or device security protocols.

Any breach of this policy may result in:

- Withdrawal of access rights for learners (which may lead to termination of our services).
- Disciplinary action for employees, up to and including dismissal.
- Termination of contracts for self-employed contractors.
- Reporting to the relevant authorities where a breach of law or regulation has occurred.

All cases of non-compliance will be investigated by the Directors to determine the severity of the breach and appropriate corrective or disciplinary action.

Monitoring and Reviewing

Pathways LDN Ltd. is committed to ensuring our policies are effective and up-to-date.

The Directors are responsible for this process and will review this policy at least once a year or more frequently if needed due to changes in laws, regulatory guidance, or best practice.