PWL PATHWAYS LDN
Employment, Skills & Training

E-Safety and Acceptable Use Policy

Version 2.0

Contents

Version Control

Version	Reviewer Name	Date	Next Review	Comments
1.0	Rena Panesar	Sept 2024	Sept 2025	First Policy.
2.0	Policy Pros	Oct 2025	Oct 2026	Retemplated and updated to include broader Acceptable Use and E-Safety.

Introduction

Pathways LDN is committed to providing a quality-enriched learning journey and promoting the professional use of technology. We recognise the immense benefits that digital technologies offer to teaching and learning, enhancing skills, and promoting lifelong learning. However, the accessibility and global nature of the internet mean we are equally committed to managing the potential risks and challenges associated with digital access.

We implement appropriate safeguards while supporting staff and learners to identify and manage digital risks independently and with confidence. This policy ensures we satisfy our duty of care.

Purpose

The purpose of this policy is to:

- Ensure full compliance with the statutory duties under Keeping Children Safe in Education (KCSIE 2025) and the Prevent Duty Guidance regarding online safety and appropriate filtering and monitoring.
- Establish and maintain robust technical and procedural safeguards to protect staff, learners, and the company from online harm, cyber threats, and the misuse of data.
- Define clear rules for the acceptable and responsible use of all company and personal devices used for work/learning.
- Provide transparent procedures for identifying, reporting, and responding to e-safety incidents and disclosures of online harm.

Who and what this policy applies to

This policy applies to:

- All staff and learners.
- Use of company-provided ICT systems, networks, mobile devices, and any personally owned devices (BYOD) used for work or learning purposes.
- All activities occurring on Pathways LDN premises, at employer/placement sites (for apprentices), and through company-approved digital learning platforms.

Definitions

E-safety: protecting learners, staff and data when using digital technologies, including safe behaviour online, secure handling of information, and responsible use of systems and devices.

E-safety incident: any event where the use of technology endangers personal safety, mental well-being, or financial well-being, or breaches the rules of acceptable use.

Systems: the software and services Pathways LDN uses to deliver and support learning, for example, email, learning platforms, file storage, video tools, and authentication services.

Networks: the wired and wireless infrastructure that connects users and systems, including internet access, routers, switches, firewalls, and any remote access used for work.

Devices: any equipment used to access Pathways LDN systems or data, for example, desktops, laptops, tablets, smartphones, and removable media, whether owned by the company, employer, or the staff member/learner.

Legal Framework

- Online Safety Act 2023
- Data Protection Act 2018 and UK GDPR
- Computer Misuse Act 1990
- Communications Act 2003 section 127
- Malicious Communications Act 1988
- Protection from Harassment Act 1997
- Equality Act 2010
- Human Rights Act 1998
- Defamation Act 2013
- Copyright, Designs and Patents Act 1988
- Protection of Children Act 1978 and Criminal Justice Act 1988 section 160
- Sexual Offences Act 2003 and Voyeurism (Offences) Act 2019
- Domestic Abuse Act 2021 and Criminal Justice and Courts Act 2015 section 33
- Counter-Terrorism and Security Act 2015
- The Telecommunications (Lawful Business Practice) Regulations 2000
- Health and Safety at Work etc. Act 1974 and the Management of Health and Safety at Work Regulations 1999

Roles and Responsibilities

Directors

- Set the e-safety policy, approve controls, and provide resources, training, and monitoring.
- Assign a senior lead for e-safety, incident response, and data protection.
- Ensure filtering, monitoring, access control, and safeguarding are in place across systems, networks, and devices.
- Review incident reports, audit results, and lessons learned, and authorise improvements.
- Make sure partner agreements and BYOD rules include e-safety and data security requirements.

Delivery staff

- Use approved platforms and follow e-safety, safeguarding, and data protection procedures.
- Brief learners on online conduct, privacy, and reporting routes at the start of a course/program.
- Check identity for live online sessions, manage waiting rooms, and control recording with consent.
- Report concerns or incidents immediately and preserve evidence.
- Keep devices patched and protected, use strong passwords and MFA, and store data only in approved locations.

Employers

- Provide a safe digital environment for apprentices and placement learners, including suitable filtering and supervision.
- Confirm local IT rules during induction and supply required software, accounts, and training.
- Protect learner data, restrict access to a need-to-know basis, and report incidents to Pathways LDN without delay.
- Support reasonable adjustments, for example, accessible software or assistive tech where needed.

Learners

- Follow online conduct rules, use respectful language, and protect personal information.
- Use only approved accounts and platforms for learning and keep passwords secret.
- Do not record sessions or share content without permission.
- Report harmful content, bullying, or technical concerns to a tutor at once.
- Keep personal devices secure with updates, screen locks, and antivirus software when used for learning.

Policy

The 4 C's of Online Safety

Pathways LDN frames its online safety education around the four areas of risk identified in statutory guidance: Content, Contact, Conduct, and Commerce.

Content

Content is anything posted online—words, images, or videos. We recognise the risk when learners may see illegal, inappropriate, or harmful content.

- This includes material related to pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- Learners are taught to identify misinformation, disinformation, and conspiracy theories as forms of harmful content that can draw individuals towards extremist views and are encouraged to question the validity of online sources.

Contact

Contact involves the risk of harm that learners may face when interacting with other users online.

- This includes situations where predators pose as children or vulnerable adults with the intention of grooming or exploiting another person for sexual, criminal, financial, or other purposes.
- Contact risks also include harmful interactions like child-on-child abuse, bullying, harassment, radicalisation, or being exposed to inappropriate commercial advertising.

Conduct

Conduct means the way people behave online.

- Unacceptable online behaviour that increases the likelihood of, or causes, harm, such as online bullying or making inappropriate and offensive comments. Conduct also includes high-risk behaviours like sharing or receiving nudes and semi-nude images (sexting) and viewing or sending pornography.

- Learners are educated on the severe legal and personal consequences of these actions.

Commerce

Commerce is about the risk of financial and commercial exploitation online.

- This covers risks such as online gambling, phishing, or financial scams.
- We ensure staff and learners are aware of how the risk from commerce applies to them, covering matters like inappropriate advertising and financial scams targeted through work communication channels.

Risk-Assessing Online Platforms

Pathways LDN commits to a proactive risk assessment of all digital services to protect our learners.

- All external online platforms, learning environments, and collaboration tools used by learners must first undergo a risk assessment by the E-Safety Officer.
- The risk assessment verifies the platform's suitability based on:
    - data security protocols;
    - age restrictions;
    - content moderation policies;
    - privacy settings;

  ensuring they do not breach our wider data protection or safeguarding standards.
- Every new platform or digital activity used by learners is risk-assessed against the 4 C's to ensure it is deemed low-risk before use is approved.
- At present, all of the online platforms used are low risk.

Appropriate Online Behaviour

All communication conducted via digital means must be professional, respectful, and adhere to the same standards of conduct expected face-to-face.

Email and Communication Channels

- Staff and learners must only use professional and appropriate language in all communication. Any message written must be clear and not open to misinterpretation.
- Emails of a personal nature are not permitted on company systems or platforms.
- Online communication between staff and learners is strictly restricted to approved company networks (such as official company email or secure learning platforms). Staff must not use personal phones, emails, or social media accounts to contact learners.
- All staff and learners are reminded that emails are subject to Freedom of Information requests and must be written with the understanding that they may be disclosed.

Video Meetings (Virtual Classroom)

- Staff and learners should ensure they are in a private environment when attending video meetings and should be mindful that backgrounds in videos do not share any personal information or inappropriate content.
- For online training, our policy encourages learners to have cameras turned on to help ensure they are in a safe environment and not vulnerable to abuse or harm. However, staff will provide guidance on how to turn cameras off if they prefer.
- Staff and learners will be mindful of language and general conduct, recognising that acceptable behaviour can be misinterpreted digitally.
- All attendees are required to be suitably dressed when appearing on camera, avoiding overly revealing clothing and clothing with slogans or images that could cause offence.
- Staff must maintain professional boundaries at all times.

Acceptable Use and Digital Values

Adherence to our Acceptable Use standards is mandatory for all accessing our digital environments.

- All staff and learners will be made aware of all relevant policies, Codes of Conduct, etc., upon induction and through ongoing training.
- Learners are responsible for using Pathways LDN's IT devices and systems safely and sensibly whilst abiding by our Acceptable Use rules (as detailed in the learner induction pack).
- Staff are responsible for consistently displaying a model example of good digital practice to learners at all times.

Our Digital Code of Conduct

- **Protect Passwords:** Ensure passwords are strong and never shared.
- **Maintain Boundaries:** Maintain clear boundaries between personal and professional online activities.
- **Share Cautiously:** Nobody's information should be shared without their explicit permission.
- **Respect Rights:** Observe copyright and referencing rules.
- **Think Before We Post!** Act with integrity and have respect for others in online communities.
- **Think Before We Type!** Only use professional and appropriate language; ensure nothing written is open to misinterpretation.
- **Think Before We Click!** Do not download anything or open any link unless confident that it is safe.
- **Stick to Policy:** Follow all company guidelines for the use of ICT and social media.
- **Report It!** Inform the DSL/E-Safety Officer of any incidents and/or concerns immediately.
- **Committed to Improve:** Display commitment to improving digital literacy skills and keeping up to date with changing e-safety requirements.

Prohibited Conduct (Unacceptable Use)

All users must ensure their digital conduct complies with UK law and company policy. Prohibited conduct includes, but is not limited to:

- Using any digital system to bully, harass, intimidate, or victimise any individual, including cyber-bullying.
- Posting any content that is defamatory, malicious, or false about Pathways LDN, its staff, learners, or partners, or any content designed to bring us into disrepute.
- Sharing or accessing any images, rhetoric, or materials that are discriminatory, hateful, or extremist in nature (e.g., related to racism, misogyny, homophobia, or radicalisation).
- Downloading, uploading, or distributing copyrighted materials (music, films, or resources) without proper permission or license, and ensuring proper citation where required.
- Accessing, sharing, or attempting to breach the security of personal data or sensitive information belonging to learners, staff, or the company, in violation of the UK GDPR and our Data Protection and GDPR Policy.
- Attempting to gain unauthorised access to any system (hacking), deliberately installing malware or viruses, or engaging in any other activity that violates the Computer Misuse Act 1990.

Filtering, Monitoring, and Security

Effective filtering and monitoring are mandatory statutory duties under Keeping Children Safe in Education (KCSIE 2025) to ensure learners are protected from accessing harmful and illegal online material.

- Appropriate filtering and monitoring systems are applied to the office/centre Wi-Fi, all company-owned devices (laptops, tablets, etc.), and any network accessed by staff or learners. These systems are configured to meet the Department for Education's current Cyber Security Standards.
- We will proactively work with employers to ensure they understand their responsibility to put appropriate filtering and monitoring safeguards in place for apprentices accessing the internet at the workplace, in line with safeguarding duties.

- Filtering profiles are managed to be proportionate to the user's role and risk profile (e.g., staff vs. learners). The systems must log and flag potential safeguarding incidents and persistent attempts to access prohibited content.
- Where Pathways LDN provides access to generative artificial intelligence (AI) products and systems, these will be safely managed in line with new DfE guidance. In addition, we will work with learners on how to safety use AI to maintain a positive online reputation, preparing them for their professional life.
- We will ensure that all "flagged" searches and/or the action of accessing harmful content are immediately reported to the Directors. The user will also be alerted to the breach and signposted to appropriate guidance and support resources.

Despite filtering, we will encourage learners to question the validity and reliability of materials researched, viewed, or downloaded, and to apply critical thinking skills to online content, as these skills are essential for long-term safety.

Professional Development and Policy Maintenance (E-Safety Officer)

The E-Safety Officer, Rena Panesar (Director), holds a critical responsibility for ensuring that Pathways LDN's E-Safety Policy and practices remain current, effective, and compliant. Given the constant evolution of technology and online risks, maintaining continuous professional development (CPD) is mandatory for this role.

The E-Safety Officer will:

- Undertake specialised, high-level training (e.g., DSL training updates, certified online safety courses), which is updated as required.
- Regularly reviewing updates to statutory guidance, including Keeping Children Safe in Education (KCSIE), the Prevent Duty Guidance, and new codes of practice issued by the Information Commissioner's Office (ICO) regarding data security and online risk management.
- Engage with local safeguarding partnerships and professional networks within the FE and training sector to understand emerging local threats (e.g., specific exploitation trends or new social media harms).
- Maintain a keen interest in new consumer and educational technologies, particularly those involving Generative AI and new social media platforms, to proactively assess their associated risks before they are adopted or widely used by learners.

Policy Review and Dissemination

The E-Safety Officer uses this CPD to drive continuous improvement by:

- Leading a formal review and update of this policy and related policies/guidance at least annually, or immediately following a serious incident or major legislative change.
- Designing and delivering the internal staff training programme, ensuring content reflects the latest identified risks (such as misinformation or sextortion) and practical procedures for the team.
- Reporting regularly to the Senior Management Team on emerging e-safety risks, incident trends, and the efficacy of current filtering and monitoring controls.

Incident Reporting Procedures

- Any e-safety incident must be reported to the **Directors (who act as our Designated Safeguarding Leads)** immediately. Their contact details are:
    - Email: Paul@pathwaysldnltd.com Tel: 07508114160
    - Email: Rena@pathwaysldnltd.com Tel: 07982906672
- The Directors will log all incidents and decide on the most appropriate course of action, which may involve disciplinary action or referral to external agencies.
- Any incident involving a serious safeguarding risk (e.g., grooming, illegal image sharing) will result in an immediate referral to the Police and the Local Authority Designated Officer (LADO).

Non-Compliance

Any breach of this policy, including the misuse of ICT systems, failure to report an incident, or viewing/sharing inappropriate material (including non-consensual images or extremist content), will be treated as a serious disciplinary matter.

Depending on the severity of the offence, this may lead to disciplinary action, including summary dismissal for gross misconduct or termination of the learner's program.

Monitoring

The E-Safety Officer, supported by the Senior Management Team, is responsible for monitoring the effectiveness and compliance of our E-Safety provision through the following methods:

- Periodically reviewing the technical effectiveness of filtering and monitoring provisions (at least annually) to ensure that the systems meet current DfE standards and are working as expected on all company-owned devices and networks.
- Regularly auditing filtering and monitoring system logs to identify trends in attempted access to prohibited content, unusual user activity, and compliance breaches. This data is used to justify and refine filtering settings.
- Systematically analysing all logged e-safety incidents (reported via the incident report form) to identify patterns, repeat offenders, or emerging threats (e.g., a rise in specific types of cyberbullying or phishing attempts).
- Tracking staff completion rates for mandatory e-safety and Prevent training to ensure all personnel are equipped with the knowledge to uphold the policy.

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.

This policy will be made available in other formats upon request, and all learners are encouraged to speak to any member of staff if they have any questions or require clarification.