

Staff IT, Communications and Generative AI Acceptable Use Policy and Procedure

Academic year 2026–2027



LIMISHA

TRAINING ACADEMY

Hair • Beauty • SEND Provision

Contents

Contents	2
1. Purpose.....	3
2. Scope	3
3. Key principles	3
4. Account and device security	3
5. Communication with learners.....	3
6. Safeguarding and online safety	4
7. Prohibited use	4
8. Generative artificial intelligence	4
9. Data protection, confidentiality and records	5
10. Approved systems, platforms and storage.....	5
11. Reporting IT, communication, online safety and AI concerns	5
12. Monitoring and review	5
13. Staff declaration	5

Staff IT, Communications and Generative AI Acceptable Use Policy and Procedure

1. Purpose

This policy sets the standards for safe, lawful and professional use of Limisha Training Academy IT systems, accounts, devices, communications, online platforms, cloud services and generative AI. As an alternative provision, the Academy works with learners who may have varied needs, vulnerabilities, placements or placement arrangements, so staff must use technology in a way that supports safeguarding, online safety, data protection, confidentiality, professional boundaries and appropriate information sharing.

2. Scope

This policy applies to all staff, tutors, volunteers, agency workers, contractors, consultants and visitors who use Limisha Training Academy systems or communicate on behalf of the Academy. It applies on site, off site, during outreach, alternative provision delivery, work-related travel, remote learning, online delivery and home working. It covers Academy devices, Academy accounts, approved platforms and any personal device or account used for approved work purposes.

3. Key principles

Staff must use technology in a way that is safe, lawful, necessary, proportionate, professional and capable of audit. Staff must protect personal information, maintain professional boundaries, follow safeguarding and data protection procedures, and use only approved systems for Limisha Training Academy business. Where learners are placed through a school, local authority or partner, relevant IT, attendance, welfare, safeguarding and communication information must be shared only through agreed Academy channels.

4. Account and device security

Staff must use individual accounts and must never share passwords, authentication codes, security tokens or access to Academy systems. Strong, unique passwords and multi-factor authentication must be used where available. Screens must be locked when unattended and devices must be stored securely.

Loss, theft, suspected compromise, malware, unauthorised access or accidental disclosure must be reported immediately to a senior leader and the person responsible for IT or data protection. Staff must not install unapproved software, bypass filtering or monitoring, alter security settings, connect unknown storage devices, or use unapproved personal cloud storage for Academy information.

5. Communication with learners

Communication with learners must be professional, necessary, appropriate to the learner's age and needs, and capable of audit. Staff must use approved Academy accounts and channels only. Personal social media accounts, disappearing messages, encrypted private chats, gaming platforms, secret conversations and personal email accounts must not be used to communicate with learners.

- Keep messages clear, respectful, work-related and free from informal, intimate or suggestive language.
- Copy or record significant communication where safeguarding, case management, attendance, behaviour, welfare or complaint procedures require it.

- Do not photograph, video or record learners on personal devices.
- Do not accept or send personal friend, follow or connection requests with learners.
- Report any boundary concern, inappropriate message, online harm or safeguarding concern to the Designated Safeguarding Lead without delay.

6. Safeguarding and online safety

- Learners under 18 must be treated as children for safeguarding purposes. Staff must follow the Academy Safeguarding and Child Protection Policy and report concerns to the Designated Safeguarding Lead without delay.
- For learners aged 18–25, staff must consider adult and transitional safeguarding where there are concerns about vulnerability, exploitation, abuse, neglect, coercion, mental capacity or welfare risk.
- Staff must recognise online risks including harmful content, unsafe contact, bullying, harassment, exploitation, grooming, scams, radicalisation, misinformation, AI-generated abuse, deepfakes and image-based abuse.
- Filtering and monitoring arrangements for Academy-controlled systems must have named senior leadership oversight, supported by safeguarding and IT support. Their effectiveness must be checked, recorded and reviewed at least annually and whenever there is a significant technology, risk or delivery change.

7. Prohibited use

Academy systems, devices, accounts and networks must not be used to access, create, store, send or share illegal, extremist, discriminatory, abusive, hateful, harassing, sexual, exploitative, unsafe or otherwise inappropriate material. Staff must not use Academy systems for cyberbullying, intimidation, impersonation, unauthorised surveillance, gambling, fraud, commercial activity, political campaigning, copyright infringement or personal business.

Staff must not attempt unauthorised access, extract data without approval, disable security controls, upload confidential or personal data to unapproved websites, apps or AI tools, or use technology in a way that could place learners, colleagues, families, schools, placing organisations, partners or the Academy at risk.

8. Generative AI

Generative AI may only be used for Academy work where the tool and use have been approved and are lawful, safe, proportionate, transparent, age appropriate and suitable for education. AI outputs must be treated as drafts and checked by a competent person for accuracy, bias, safeguarding implications, copyright, data protection, accessibility, equality and suitability before use. AI must not replace professional judgement, safeguarding decisions, assessment judgement or direct learner support.

- Do not enter identifiable learner, staff, safeguarding, medical, special category, assessment, disciplinary, attendance, case-management or commercially confidential information into public or unapproved AI systems.
- AI must not make final decisions about safeguarding, admissions, discipline, assessment, support, risk, referrals, employment or learner suitability.
- Generated content must not be presented as verified evidence, professional judgement, original learner work or a factual record unless checked and properly recorded.

- Material AI assistance must be disclosed in formal reports, learning materials, policies, assessments or communications where transparency is required.
- AI-generated images, audio, video, deepfakes or impersonation content involving learners, staff or third parties must be treated as a safeguarding and conduct risk and reported immediately.

9. Data protection, confidentiality and records

Personal data must be processed lawfully, fairly and securely. Staff must only access, record, share or retain information where there is a legitimate work reason, safeguarding reason, legal obligation or agreed education purpose. Confidential information must be stored only in approved Academy systems and shared only with authorised people using approved channels. Records about safeguarding, attendance, behaviour, welfare, support, medical needs, special category information, incidents, placement updates and AI use must be accurate, factual, dated and retained in line with Academy procedures.

Personal data must not be entered into public or unapproved AI tools. Where AI is approved for Academy use, staff must use the minimum necessary information, avoid identifiable details unless specifically authorised, check outputs carefully, and record material AI use where it affects formal records, reports, learner support, safeguarding, assessment or communication with external agencies.

10. Approved systems, platforms and storage

Academy information must be created, stored and shared using approved systems only. Staff must not use personal email, personal cloud accounts, personal messaging apps or unapproved file-transfer services for Academy records. Where a new app, website, AI tool or online service is proposed, it must be checked before use for safeguarding suitability, data protection, security, age appropriateness, accessibility, contractual terms and record-keeping requirements.

11. Reporting IT, communication, online safety and AI concerns

Staff must report any IT security incident, data protection concern, inappropriate communication, online safety issue, AI-related concern, suspected misuse of systems, professional boundary concern or safeguarding concern without delay. Safeguarding concerns must be reported to the Designated Safeguarding Lead in line with Academy procedures. Data breaches or suspected data breaches must be escalated to the person responsible for data protection. Evidence must be preserved where safe to do so.

12. Monitoring and review

Limisha Training Academy will review this policy at least annually and sooner where there are significant changes to statutory safeguarding guidance, online safety, filtering and monitoring expectations, data protection requirements, generative AI guidance, technology or Academy practice. For the 2026–2027 academic year, practice will reflect Keeping Children Safe in Education 2025 until 31 August 2026 and Keeping Children Safe in Education 2026 from 1 September 2026.

Limisha Training Academy may monitor use of Academy systems, accounts, devices and platforms for safeguarding, security, compliance, investigation and operational purposes in a proportionate and transparent way. Staff should not expect personal privacy when using Academy systems, although monitoring information will be handled securely and in line with data protection requirements.

13. Staff declaration

I confirm that I have received, read and understood the Limisha Training Academy Staff IT, Communications and Generative AI Acceptable Use Policy and Procedure for the 2026–2027 academic year. I agree to follow the standards in this policy and understand that failure to do so may result in support, training, management action, disciplinary action, referral to external agencies or ending my working arrangement, depending on the seriousness of the matter.

I understand that safeguarding is everyone's responsibility and that I must report any safeguarding, online safety, IT security, data protection, communication, AI-related or professional boundary concern promptly and in line with Academy procedures.

Staff member name	
Role / position	
Signature	
Date	