



ICT, Online Safety and Acceptable Use Policy

Secondary Alternative Education Provision

Policy Owner	In-Tuition Learning
Effective Date	August 2026
Review Date	August 2027

Our commitment

In-Tuition Learning uses digital technology to support safe, inclusive and effective learning. All users are expected to use systems lawfully, securely, respectfully and in a way that protects learners, staff, information and the organisation.

Contents

- 1. Purpose and scope
- 2. Age range and application
- 3. Roles and responsibilities
- 4. Core acceptable-use expectations
- 5. Accounts, passwords and access
- 6. Devices, software and storage
- 7. Internet, filtering and monitoring
- 8. Communication, social media and online conduct
- 9. Remote learning and live online tuition
- 10. Online safety and safeguarding
- 11. Artificial intelligence and emerging technology
- 12. Data protection, confidentiality and copyright
- 13. Cyber security and incident response
- 14. Personal devices and bring your own device
- 15. Monitoring, sanctions and review
- 16. Related policies
- Appendix 1 - Learner acceptable-use agreement
- Appendix 2 - Staff and contractor acceptable-use agreement
- Appendix 3 - Digital incident response checklist

1. Purpose and scope

This policy sets out how In-Tuition Learning provides and uses digital technology safely and responsibly. It replaces the previous one-page acceptable-use summary and applies to organisation-owned devices, accounts, networks, cloud services, learning platforms, email, messaging, remote tuition and any personal device used for organisational work.

It applies to learners, staff, tutors, volunteers, contractors, visitors and any other authorised user. Access to systems is conditional on compliance with this policy and any linked acceptable-use agreement.

Technology supports learning

Controls should be proportionate and should enable learning, communication and reasonable adjustments. They must not be used as a substitute for supervision, professional judgement or safeguarding practice.

2. Age range and application

In-Tuition Learning may teach learners of secondary-school age and young adults up to age 25. Online-safety and acceptable-use expectations apply to every learner. Safeguarding concerns involving a learner under 18 are managed under child-protection procedures; concerns involving an adult learner are managed through appropriate adult-safeguarding, police or other support routes where relevant.

3. Roles and responsibilities

Role	Key responsibility
Director	Approves this policy, ensures appropriate resources and oversight, reviews significant incidents and determines organisational action.
Designated Safeguarding Lead	Leads on online-safety safeguarding concerns, coordinates referrals and reviews filtering or monitoring information where it indicates risk.
IT support / service provider	Maintains systems, access controls, updates, backups, filtering, security tools and technical incident support within the agreed service.

Role	Key responsibility
Staff and tutors	Model safe use, supervise learners, protect information, report concerns promptly and follow approved platforms and procedures.
Learners	Use systems for authorised purposes, respect others, protect account details and report anything unsafe, harmful or suspicious.
Parents, carers and commissioners	Support agreed arrangements, share relevant risks and raise concerns through appropriate channels.

4. Core acceptable-use expectations

- use systems only for authorised educational or organisational purposes
- communicate respectfully and never harass, threaten, discriminate against or impersonate another person
- do not create, access, store or share illegal, abusive, sexual, hateful, violent or otherwise harmful material
- do not attempt to bypass security, filtering, monitoring or access restrictions
- do not damage equipment, interfere with services or use another person’s account
- report accidental access to harmful content, suspicious messages, lost devices or other concerns immediately
- follow staff instructions and any individual risk-management or reasonable-adjustment plan
- understand that use of organisational systems may be logged and reviewed for safeguarding, security and operational purposes

5. Accounts, passwords and access

- Each user must use their own authorised account and must not share passwords or authentication codes.
- Passwords must be strong, unique and changed immediately where compromise is suspected.
- Multi-factor authentication will be used where available and proportionate.
- Users must lock or sign out of devices when unattended and must not leave confidential information visible.
- Access rights will be limited to what is necessary and removed promptly when no longer required.
- Administrator accounts must be restricted and used only for authorised technical tasks.
- Shared accounts should be avoided; where unavoidable, ownership, access and review arrangements must be documented.

6. Devices, software and storage

- Treat all equipment carefully and report damage or faults promptly.
- Do not install software, browser extensions or applications without approval.
- Do not disable security tools, updates, encryption, device management or other controls.
- Store organisational information only in approved locations and services.
- Portable storage devices must be approved, encrypted where appropriate and checked for malware.
- Devices must not be left unsecured in vehicles, public places or unattended learning spaces.
- Confidential printing must be collected promptly and disposed of securely.
- Organisation-owned devices may be inspected, updated, remotely managed or wiped where necessary.

7. Internet, filtering and monitoring

In-Tuition Learning will use proportionate filtering and monitoring arrangements on networks and devices it controls. Filtering is intended to prevent access to illegal, inappropriate or harmful material. Monitoring supports the identification and review of concerning activity; it does not replace active supervision.

- Filtering and monitoring controls will reflect the age, needs and vulnerability of learners, including SEND and reasonable adjustments.
- Known over-blocking or under-blocking will be reviewed so that legitimate learning is not unnecessarily restricted.
- Users must not use proxy services, virtual private networks, alternative DNS services or other methods to bypass controls unless specifically authorised.
- Alerts and logs will be reviewed by an appropriate person and escalated where they indicate safeguarding, criminal, cyber-security or welfare concerns.
- Filtering and monitoring arrangements will be checked at least annually and after significant changes or incidents.
- Use of personal mobile data does not remove the requirement to follow this policy.

Privacy and monitoring

Users should not expect personal privacy when using organisational systems. Monitoring will nevertheless be lawful, proportionate, transparent and limited to legitimate safeguarding, security, compliance and operational purposes.

8. Communication, social media and online conduct

- Use approved professional accounts and platforms for communication with learners.
- Do not use personal social-media accounts to contact learners or accept friend or follow requests where this would blur professional boundaries.
- Messages must be appropriate, necessary and capable of professional scrutiny.
- Do not record, photograph, screenshot or share lessons, meetings, learners or staff without permission and a lawful purpose.
- Do not publish confidential information, personal data or content that could identify a learner without authorisation.
- Do not post content that could reasonably damage trust, safety or the reputation of learners, staff, partner organisations or In-Tuition Learning.
- Cyberbullying, abusive messages, malicious rumours, doxxing and non-consensual sharing are prohibited.

9. Remote learning and live online tuition

- Only approved platforms and accounts may be used.
- Session links, passwords and meeting details must not be shared beyond authorised participants.

- Staff should work from an appropriate location and protect confidential information visible or audible in the background.
- Learners should use suitable names and settings and must not record or redistribute sessions without permission.
- Unexpected adults, inappropriate behaviour, harmful material or safeguarding disclosures must be managed in line with safeguarding procedures.
- One-to-one online tuition must follow the same professional-boundary expectations as face-to-face provision.
- Where a session becomes unsafe or unmanageable, staff may pause or end it and must record and report the reason.

10. Online safety and safeguarding

Online safety is part of safeguarding. Staff must report concerns rather than investigate them.

Relevant risks include:

- grooming, coercion, exploitation and unwanted contact
- sexual harassment, sexualised bullying and the sharing of nude or semi-nude images
- self-harm, suicide, eating-disorder and other harmful content
- radicalisation, extremist material and hateful content
- fraud, scams, financial exploitation and identity theft
- cyberbullying, stalking, impersonation and reputational harm
- violent content, dangerous challenges and instructions for harmful acts
- location sharing, oversharing and loss of privacy
- compulsive use, sleep disruption and effects on wellbeing

Where there is immediate danger or a suspected serious crime, call 999. Preserve relevant evidence where safe to do so, but do not search devices or accounts beyond what is necessary and authorised.

11. Artificial intelligence and emerging technology

- AI tools may be used only where approved and appropriate for the learning or work task.
- Do not enter confidential, personal, safeguarding, commercially sensitive or copyrighted material into public AI services unless specifically authorised.
- AI output must be checked for accuracy, bias, fabrication, harmful content and inappropriate disclosure.
- Learners must not present AI-generated work as wholly their own where this breaches assessment rules.
- AI must not be used to generate abusive, sexual, deceptive, discriminatory or impersonating content, including deepfakes.
- Staff remain professionally accountable for decisions, feedback, reports and communications supported by AI.
- New tools will be risk-assessed before use, including their data use, age restrictions, security and safeguarding implications.

12. Data protection, confidentiality and copyright

- Use personal data only for an authorised purpose and share it only with people who have a legitimate need to know.
- Check recipients and attachments before sending messages. Use secure transfer methods where required.
- Do not access records out of curiosity or for personal reasons.
- Report misdirected emails, lost information, unauthorised access or other possible data breaches immediately.
- Follow retention and secure-deletion requirements.
- Respect copyright, licences and intellectual-property rights. Do not copy, download or distribute material unlawfully.
- Use appropriately licensed images, music, software and learning resources and acknowledge sources where required.

13. Cyber security and incident response

- Be alert to phishing, fake login pages, unexpected attachments, QR-code scams and requests for passwords or money.
- Verify unusual requests through a separate trusted route.
- Keep software, browsers and operating systems updated.
- Do not connect unknown devices or storage media.
- Report ransomware messages, unusual pop-ups, unexplained account activity, missing files or suspected malware immediately.
- Where compromise is suspected, disconnect the affected device from the network if safe, stop using it and seek technical support.
- Do not pay, negotiate with or respond to attackers unless instructed by authorised law-enforcement or specialist advisers.
- Significant incidents will be assessed for safeguarding, data-protection, contractual, insurance and reporting implications.

Immediate cyber action

Stop, disconnect if safe, preserve evidence, report promptly and follow technical instructions. Do not continue experimenting with a compromised device or account.

14. Personal devices and bring your own device

- Personal devices may be used only where authorised and suitable for the task.
- The owner remains responsible for the device, software licensing, physical security and personal backups.
- Organisational data must not be stored permanently on a personal device unless specifically approved and protected.
- Screen locks, updates, anti-malware and encryption must be enabled where appropriate.

- Personal devices must not be used to photograph, record or contact learners outside approved arrangements.
- In-Tuition Learning may require organisational data to be removed from a personal device and may withdraw permission to use it.
- Users must separate personal and organisational accounts and avoid automatic syncing to personal cloud services.

15. Monitoring, sanctions and review

Suspected breaches will be considered fairly and proportionately. Action may include advice, additional supervision, restricted access, removal of equipment, disciplinary or behaviour procedures, notification of parents or carers, commissioners, safeguarding services, police, insurers, regulators or other relevant bodies.

The response will consider intent, impact, age, capacity, vulnerability, previous concerns, safeguarding context and any reasonable adjustments. Access may be suspended immediately where necessary to protect people, information or systems.

- significant incidents and emerging patterns
- effectiveness of filtering, monitoring and technical controls
- staff and learner training needs
- new platforms, AI tools and cyber threats
- changes to law, guidance, contracts or commissioning requirements
- feedback from learners, parents, carers and staff

16. Related policies

- Safeguarding and Child Protection Policy
- Prevent and Radicalisation Policy
- Data Protection and Privacy Policy
- Staff Code of Conduct
- Behaviour and Anti-Bullying Policy
- Equality, Diversity and Inclusion Policy
- Complaints and Appeals Policy
- Health and Safety Policy
- Remote Tuition and Lone Working arrangements
- Assessment and Academic Integrity procedures

Appendix 1 - Learner acceptable-use agreement

I understand that access to In-Tuition Learning technology is provided for learning and agreed activities. I agree that I will:

- use my own account and keep my password private
- treat devices and equipment carefully
- communicate respectfully and not bully, threaten or impersonate anyone
- not access, create or share illegal, sexual, violent, hateful or otherwise harmful material
- not bypass security, filtering or monitoring
- not record or share lessons, staff or other learners without permission
- protect personal information and report anything that makes me feel unsafe or uncomfortable
- tell a member of staff immediately if I see harmful content, receive suspicious contact or make a mistake online
- use AI honestly and follow assessment instructions
- accept that use of organisational systems may be logged and reviewed

I understand that access may be restricted or removed if I do not follow this agreement and that serious concerns may be shared with parents, carers, commissioners, safeguarding services or police where appropriate.

Field	Completion
Learner name	
Signature	
Date	
Parent / carer name and signature, where appropriate	

Appendix 2 - Staff and contractor acceptable-use agreement

I confirm that I will:

- use approved accounts, devices, platforms and storage locations
- maintain professional boundaries in all digital communication
- protect passwords, authentication codes and confidential information
- not use personal accounts or devices for learner contact unless expressly authorised
- report safeguarding, cyber-security and data-protection concerns immediately
- not disable, bypass or undermine technical safeguards
- use AI and cloud services only in accordance with this policy
- comply with copyright, licensing and assessment-integrity requirements
- return equipment and remove organisational data when access ends
- cooperate with proportionate monitoring and incident investigation

Field	Completion
Name	
Role / organisation	
Signature	
Date	

Appendix 3 - Digital incident response checklist

Stage	Required action
1. Make safe	If anyone is in immediate danger, call 999. Stop the activity and remove access only where safe and authorised.
2. Preserve evidence	Do not delete relevant messages, logs or files. Record dates, times, usernames, devices and what was observed.
3. Contain	For a cyber incident, disconnect the affected device if safe. Change compromised credentials using a clean device when advised.
4. Report	Tell the Director, DSL or appropriate technical contact immediately according to the nature of the incident.
5. Assess	Consider safeguarding, crime, data breach, system security, business continuity and contractual implications.
6. Notify	Contact relevant services, commissioners, parents or carers, insurers, regulators or police where required and lawful.
7. Recover	Follow technical advice, restore from trusted backups, verify security and communicate any temporary arrangements.
8. Review	Record decisions, support affected people, identify lessons and update controls, training or risk assessments.