ELEVATED

A Holistic Approach
To The Education of Young People

ICT User Acceptance Policy

Date Adopted: 9th September 2025

Review Date: September 2026

Policy Lead: Mark Aitken - Head of Provision

1. Statement of Intent

ElevatEd AP Ltd is committed to ensuring that all users of ICT systems — including students, staff, volunteers, and visitors — use technology safely, responsibly, and in line with our values. ICT is central to teaching, learning, communication, and safeguarding. This policy sets out clear rules to protect users, safeguard data, and promote digital wellbeing.

2. Guiding Principles

- ICT is a tool to support learning, creativity, and wellbeing.
- Users must act with integrity, respect, and responsibility.

- ICT must be used in a way that keeps children and staff safe online and offline.
- Personal data and information must always be protected.
- Misuse of ICT may lead to disciplinary action, safeguarding intervention, or legal action.

3. Scope This policy applies to:

- All users of ElevatEd's ICT systems (students, staff, parents, volunteers, contractors).
- All ICT devices (PCs, laptops, tablets, smartphones, printers, projectors).
- All networks, internet access, and software systems.
- Personal devices when connected to ElevatEd's network or used for ElevatEd business.

4. Definitions

- ICT: Information and Communication Technology, including hardware, software, and online systems.
- User: Any person authorised to use ElevatEd ICT systems.
- Acceptable Use: Safe, responsible, and educationally beneficial use of ICT.
- Unacceptable Use: Misuse of ICT that is unsafe, illegal, harmful, or breaches this policy.

5. Roles and Responsibilities

- Leadership Team: Ensure robust ICT safety policies, resources, and monitoring systems.

- Data Protection Officer (DPO): Maintain systems securely, monitor usage, and respond to breaches.
- Staff: Model responsible ICT use, supervise students, and report concerns promptly.
- Students: Follow the rules of this policy and respect ICT equipment.
- Parents/Carers: Support their child in safe, responsible ICT use at home.

6. Acceptable Use Rules

For Students:

- Use ICT only for learning and creativity.
- Always log in with your own username and keep passwords private.
- Respect others — no cyberbullying, harassment, or inappropriate communication.
- Report any harmful or unsafe content to a member of staff immediately.
- Treat equipment with care.

For Staff/Adults:

- Use ICT only for professional purposes in line with ElevatEd values.
- Protect student data in line with the Data Protection Policy.
- Do not use ICT for personal gain, inappropriate material, or illegal activity.

- Maintain professional boundaries online (including social media).
- Report any ICT misuse or breach immediately.

7. Unacceptable UseExamples include (but are not limited to):

- Accessing, downloading, or sharing offensive, extremist, or illegal content.
- Bypassing security or attempting unauthorised access (“hacking”).
- Using ICT to bully, harass, or harm others.
- Sharing confidential information without authorisation.
- Damaging or misusing equipment, software, or systems.
- Using ICT for personal commercial purposes.

8. ICT Monitoring and Filtering

- ElevatEd monitors ICT use for safeguarding, security, and compliance.
- Internet access is filtered to block harmful content.
- Email and digital communication may be monitored where safeguarding concerns arise.
- Users should have no expectation of privacy when using ElevatEd ICT systems.

9. Reporting ICT Misuse

All users must report ICT misuse immediately to a staff memberReporting ICT Misuse

Step 1: Misuse Detected

- Student, staff, or system identifies ICT misuse.

Step 2: Report Immediately

- Inform E Safety Lead / DSL (if safeguarding concern).

Step 3: Initial Response

- ICT access may be suspended while incident is investigated.

Step 4: Assessment

- E Safety Lead and DPO investigate the nature of misuse.
- DSL consulted if safeguarding issue.

Step 5: Action Taken

- Minor misuse → Warning / Restorative action.
- Serious misuse → Parental involvement / Disciplinary process.
- Illegal misuse → Police and external agencies informed.

Step 6: Record & Review

- Incident logged.
- Systems/policies updated to prevent recurrence.

10. Consequences of Breach

- Students: Loss of ICT privileges, parental involvement, disciplinary action, safeguarding referrals.

- Staff: Disciplinary action (up to dismissal), referral to regulatory bodies if required.
- All Users: Possible legal consequences for serious/illegal misuse.

11. Training and Awareness

- All staff trained annually on ICT safety and GDPR.
- Students receive regular online safety education.
- Parents supported through discussion and resources.

12. Monitoring and Review

- Policy reviewed annually or when legislation/technology changes.
- E Safety Lead and DSL report to Leadership Team any ICT incidents and emerging risks.

13. Related Policies

- Data Protection & Information Management Policy
- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- E Safety Policy