



IT ACCEPTABLE USE POLICY 2025-2026

Reviewed: April 2025
Next Review due: April 2026
Approved by the Senior Leadership Team



Table of Contents

1. Introduction.....	2
2. Aims	2
3. Scope.....	3
4. Principles.....	3
5. Roles and Responsibilities.....	3
6. Acceptable Use of IT Resources	4
7. Unacceptable Use	5
8. E-Safety Measures	5
9. Social Networking and Social Media Guidelines.....	6
10. Managing IT Misuse.....	6
11. Supporting SEN/SEMH Learners	7
12. Recording and Monitoring.....	7
13. Training	7
14. Collaboration with Stakeholders.....	8
15. Monitoring and Review	8
16. Consequences of Non-Compliance.....	8
17. Legal Framework.....	9
18. Contact.....	9
19. Related Policies.....	9

1. Introduction

Bespoke Mentoring and Training Services Limited ("the Organisation") is an alternative provision committed to supporting learners aged 6-25 with special educational needs (SEN) and social, emotional, and mental health (SEMH) needs. This IT Acceptable Use Policy outlines expectations for the safe, responsible, and inclusive use of IT resources, including social networking, social media, and online platforms, to protect learners and promote a positive digital environment.

This policy complies with the Data Protection Act 2018, the Equality Act 2010, the Computer Misuse Act 1990, and Department for Education (DfE) guidance, including *Keeping Children Safe in Education* (2024) and *Teaching Online Safety in Schools* (2019). It applies to all learners, staff, and relevant stakeholders (e.g., parents/carers, contractors) using Organisation-provided IT systems, devices, or networks, both on-site and during off-site activities (e.g., remote learning, educational trips).

2. Aims

- To ensure safe, responsible use of IT resources, including social media and social networking, by learners with SEN/SEMH.
- To promote e-safety, protecting learners from online risks such as cyberbullying, grooming, or inappropriate content.

- To foster a positive digital culture that supports learning, inclusion, and emotional well-being.
- To comply with legal and statutory obligations, including data protection and safeguarding requirements.
- To provide clear guidance and consequences for misuse of IT resources, tailored to SEN/SEMH needs.

3. Scope

This policy covers:

- Use of Organisation-provided IT systems, devices (e.g., tablets, computers), and networks.
- Social networking and social media platforms (e.g., WhatsApp, Instagram, TikTok) accessed on Organisation devices or personal devices during Organisation activities.
- E-safety measures to protect learners during online learning, on-site, and off-site activities.
- All learners aged 6-25 with SEN/SEMH, staff, and stakeholders interacting with Organisation IT resources.
- Online behaviour impacting the Organisation's community, even if conducted outside its systems (e.g., cyberbullying via personal devices).

4. Principles

- **Safety:** E-safety is prioritised to protect learners with SEN/SEMH from online harm.
- **Inclusion:** IT use is accessible, with reasonable adjustments for SEN/SEMH needs (e.g., visual aids, simplified interfaces).
- **Responsibility:** Users are accountable for their digital actions, respecting others' rights and privacy.
- **Education:** Learners receive SEN-appropriate training to navigate online environments safely.
- **Confidentiality:** Personal data is protected, per the Data Protection Policy and UK GDPR.
- **Respect:** Online interactions uphold equality, avoiding discrimination or harassment, per the Equality Act 2010.

5. Roles and Responsibilities

- **Senior Leadership Team:**
 - Oversees policy implementation, ensures e-safety compliance, and allocates resources for IT security.
 - Approves disciplinary actions for serious misuse.
- **E-Safety Coordinator:** A named staff member contact laura.davis@bespokementoring.org manages IT use, e-safety training, and incident response.
- **Designated Safeguarding Lead (DSL):**
 - Addresses e-safety incidents with safeguarding implications (e.g., grooming, cyberbullying).

- Liaises with external agencies (e.g., police, CEOP).
- **SENCO (Special Educational Needs Coordinator):**
 - Ensures IT resources and e-safety measures align with SEN/SEMH needs, per Education, Health, and Care Plans (EHCPs).
- **IT Support Staff:**
 - Maintain secure systems, monitor usage, and report misuse.
 - Implement technical safeguards (e.g., firewalls, content filters).
- **All Staff:**
 - Model responsible IT use, supervise learners, and report e-safety concerns.
 - Complete annual e-safety training, with SEN/SEMH focus.
- **Learners:**
 - Follow IT use rules, report concerns, and engage in e-safety education, with SEN/SEMH support.
- **Parents/Carers:**
 - Support e-safety at home, report concerns, and provide consent for online activities.
- **Visitors/Contractors:**
 - Adhere to IT use rules when accessing Organisation systems.

6. Acceptable Use of IT Resources

Learners are expected to:

- **Use Organisation Devices Responsibly:**
 - Access only approved platforms and resources for learning (e.g., educational apps, virtual classrooms).
 - Avoid tampering with devices, software, or settings (e.g., deleting files, installing unauthorised apps).
- **Engage Safely in Social Networking and Social Media:**
 - Use social media only during approved activities, under staff supervision, and with parental consent for under-16s.
 - Post content that is respectful, avoiding offensive, discriminatory, or harmful material.
 - Protect personal information (e.g., not sharing addresses, photos) and respect others' privacy.
- **Follow E-Safety Guidelines:**
 - Report inappropriate content, messages, or behaviour to staff immediately.
 - Avoid sharing login credentials or accessing others' accounts.
 - Use strong passwords and secure connections, as guided by staff.
- **Respect Others:**
 - Avoid cyberbullying, harassment, or discrimination, per the Anti-Bullying and Hate Crime Policy.
 - Communicate online in a manner that supports inclusion and SEMH well-being.
- **Comply with Legal Standards:**
 - Avoid accessing, sharing, or creating illegal content (e.g., extremist material, explicit images).
 - Respect copyright and intellectual property laws.

7. Unacceptable Use

The following are prohibited and may result in consequences:

- Accessing or sharing inappropriate content (e.g., violent, explicit, or discriminatory material).
- Cyberbullying, trolling, or harassing others, including via social media or messaging apps.
- Unauthorised access to systems, accounts, or data (e.g., hacking, phishing).
- Sharing personal or confidential information without consent, breaching the Data Protection Policy.
- Using IT resources for non-educational purposes during learning time (e.g., gaming, personal social media).
- Posting content that harms the Organisation's reputation or learner/staff well-being.
- Engaging in illegal activities (e.g., distributing malware, accessing extremist content).
- Using personal devices to bypass Organisation filters or monitoring systems.

8. E-Safety Measures

To protect learners with SEN/SEMH, the Organisation implements:

- **Technical Safeguards:**
 - Firewalls, content filters, and antivirus software to block harmful content.
 - Monitoring software to detect misuse, with alerts for key terms (e.g., bullying, grooming).
 - Secure Wi-Fi and encrypted platforms for online learning.
- **Access Controls:**
 - Age-appropriate restrictions on social media and apps, aligned with platform age limits (e.g., 13+ for most platforms).
 - Individual logins for learners, with SEN-accessible interfaces (e.g., simplified dashboards).
 - Supervised access to devices during learning sessions.
- **E-Safety Education:**
 - Termly workshops for learners, tailored to SEN/SEMH needs (e.g., visual guides, role-plays on cyberbullying).
 - Topics include safe social media use, recognizing online risks, and reporting concerns.
 - Integrated into mentoring sessions to build digital resilience.
- **Parental Engagement:**
 - Annual e-safety guidance sessions for parents/carers, with accessible resources (e.g., simplified leaflets).
 - Consent forms for online activities, detailing risks and safeguards.
- **Staff Training:**
 - Annual e-safety training for staff, covering SEN/SEMH vulnerabilities (e.g., impulsivity in ADHD, anxiety in SEMH).
 - Guidance on monitoring online behaviour and responding to incidents.

9. Social Networking and Social Media Guidelines

- **Approved Use:**
 - Social media is permitted only for educational purposes (e.g., group projects on approved platforms) or supervised activities (e.g., Organisation-managed accounts).
 - Learners under 16 require parental consent for social media use, per platform terms and GDPR.
- **Boundaries:**
 - Learners must not connect with staff or peers on personal social media accounts to maintain professional boundaries.
 - Posting about Organisation activities requires staff approval to protect privacy.
- **Content Standards:**
 - Posts must be respectful, inclusive, and free from discriminatory or harmful content.
 - Learners are educated on the permanence of online posts and their impact on SEMH well-being.
- **Monitoring:**
 - Organisation-managed social media accounts are moderated by the E-Safety Coordinator.
 - Inappropriate posts on personal accounts affecting the Organisation's community are addressed per this policy.

10. Managing IT Misuse

10.1 Incident Response

- **Reporting:**
 - Learners report e-safety concerns (e.g., cyberbullying, inappropriate messages) to staff, using SEN-accessible methods (e.g., visual forms, verbal reporting).
 - Staff report incidents to the E-Safety Coordinator immediately.
- **Investigation:**
 - The SEN Manager, with DSL and SENCO input, investigates within 24 hours, using SEN-appropriate methods (e.g., visual interviews).
 - Safeguarding concerns (e.g., grooming, sexting) are escalated to the DSL and external agencies (e.g., CEOP, police).
- **Consequences:**
 - **Low-Level Misuse** (e.g., unauthorized gaming): Verbal warnings, reflective tasks, or parental meetings, adapted for SEN/SEMH.
 - **Moderate Misuse** (e.g., inappropriate posts): Temporary device bans, e-safety workshops, or behaviour contracts.
 - **Serious Misuse** (e.g., cyberbullying, illegal content): Suspension, police involvement, or permanent exclusion, per the Behaviour and Learning Policy.
 - Restorative approaches (e.g., mediated apologies) are prioritized where safe, using SEN-friendly formats.
- **Support:**
 - Learners receive emotional support post-incident (e.g., counselling for SEMH needs).
 - Parents/carers are informed and involved in resolutions.

10.2 Safeguarding Incidents

- Incidents involving potential harm (e.g., grooming, extremist content) are reported to the DSL immediately.
- The DSL follows the Safeguarding Policy, involving the Local Authority Designated Officer (LADO), police, or CEOP as required.
- Learners are supported with SEN/SEMH-appropriate interventions (e.g., safe spaces, mentoring).

11. Supporting SEN/SEMH Learners

- **Accessible IT:**
 - Devices and platforms use SEN-friendly features (e.g., screen readers, high-contrast modes).
 - Social media interfaces are simplified for learners with cognitive or sensory needs.
- **Tailored E-Safety:**
 - Education addresses SEN/SEMH vulnerabilities (e.g., impulsivity, susceptibility to grooming).
 - Visual aids, simplified language, and role-plays ensure understanding.
- **Emotional Support:**
 - SEMH learners receive mentoring to manage online stress or cyberbullying impacts.
 - Safe spaces are provided for learners overwhelmed by digital interactions.
- **Individual Plans:**
 - EHCPs include e-safety strategies (e.g., supervised access for impulsive learners).
 - Plans are reviewed termly with parents/carers and the SENCO.

12. Recording and Monitoring

- **Usage Monitoring:**
 - IT systems log user activity (e.g., websites visited, messages sent), with data stored securely.
 - Alerts flag potential misuse (e.g., banned keywords, excessive non-educational use).
- **Incident Logs:**
 - E-safety incidents are recorded securely, detailing the event, response, and outcomes.
 - Safeguarding incidents are escalated per the Safeguarding Policy.
- **Data Protection:**
 - Monitoring complies with the Data Protection Policy and UK GDPR, with learner consent for data processing where required.
- **Review:**
 - The SEN Manager analyses incident logs termly to identify trends (e.g., cyberbullying spikes).
 - Findings inform training and system updates.

13. Training

- **Staff:**

- Annual e-safety training, covering SEN/SEMH risks, social media monitoring, and legal obligations.
 - New staff complete training within their first week.
- **Learners:**
 - Termly e-safety workshops, tailored to SEN/SEMH needs (e.g., visual guides, interactive scenarios).
 - Ongoing mentoring to reinforce safe online habits.
- **Parents/Carers:**
 - Annual e-safety sessions, with accessible resources (e.g., simplified guides, translations).
 - Guidance on monitoring home device use.

14. Collaboration with Stakeholders

We work with:

- **Parents/Carers:** To reinforce e-safety at home and address learner-specific risks.
- **Learners:** Through councils to co-design e-safety initiatives, with SEN support.
- **Staff:** Via feedback to improve IT systems and training.
- **External Partners:** Police, CEOP, or e-safety charities (e.g., Childnet) for guidance and incident response.
- **Referring Schools:** To align on e-safety for referred learners.

15. Monitoring and Review

- **System Audits:**
 - IT systems are audited termly for security and accessibility, with updates to filters or software.
- **Incident Analysis:**
 - Termly review of e-safety incidents to refine procedures and training.
- **Feedback:**
 - Collected from learners, staff, and parents/carers using SEN-accessible methods (e.g., visual surveys).
- **Policy Review:**
 - Every year or following significant changes (e.g., new legislation, technology trends).
 - The SEN Manager leads reviews, with Senior Leadership Team approval.

16. Consequences of Non-Compliance

- **Learners:**
 - Misuse is addressed per the Behaviour and Learning Policy, with sanctions ranging from warnings to exclusion for serious breaches.
 - SEN/SEMH support ensures fair, restorative outcomes.
- **Staff:**
 - Misuse results in disciplinary action, per the Staff Discipline, Conduct, and Grievance Policy.
- **Organisation:**
 - Non-compliance risks regulatory action (e.g., ICO fines, Ofsted scrutiny) and learner safety.

17. Legal Framework

This policy complies with:

- **Data Protection Act 2018/UK GDPR:** Secure handling of personal data.
- **Equality Act 2010:** Non-discrimination and accessibility for SEN/SEMH.
- **Computer Misuse Act 1990:** Prohibiting unauthorized system access.
- **Safeguarding Vulnerable Groups Act 2006:** Protecting learners from harm.
- **DfE Guidance:** *Keeping Children Safe in Education* (2024), *Teaching Online Safety in Schools* (2019).
- **Children Act 1989:** Safeguarding duties.

18. Contact

For e-safety concerns, reporting, or support:

SEN Manager

Email: laura.davis@bespokementoring.org

Address: Bespoke Mentoring and Training Services, Regents Walk, Newerne Street, Lydney, Gloucester, GL15 5RF.

Safeguarding concerns should be reported to:

Designated Safeguarding Lead

Email: jacqui.reddan@bespokementoring.org

External support:

- **Child Exploitation and Online Protection (CEOP):** www.ceop.police.uk
- **Ofsted:** www.gov.uk/government/organisations/ofsted, 0300 123 1231
- **Childnet:** www.childnet.com, for e-safety resources

19. Related Policies

- Safeguarding Policy
- Data Protection Policy
- Behaviour and Learning
- Equal Opportunities
- Anti-Bullying and
- SEN Policy
- Staff Discipline, C

Approval

The Senior Leadership Team has approved this policy, which is effective immediately.



3, 2025, and it is