

Compass Learning & Education

STAFF E-SAFETY & ACCEPTABLE USE POLICY



1. Purpose

Compass Learning & Education recognises that online safety is an essential element of safeguarding. Technology is increasingly central to:

- Child sexual exploitation
- Radicalisation
- Grooming
- Cyberbullying
- Data breaches

This policy sets out staff responsibilities when using technology both professionally and personally.

2. Professional Conduct

Staff must:

- Read and sign this Acceptable Use Policy annually
- Use provision-issued email accounts for all official communication
- Maintain professional boundaries in all digital communication
- Never communicate with students via personal social media accounts
- Not use personal email for provision business
- Not share confidential information via unsecured channels
- Use strong passwords and enable 2FA where possible
- Maintain appropriate privacy settings on personal accounts

Online conduct outside of work that undermines professional reputation may result in disciplinary action.

3. Safeguarding & Online Risks

Staff must:

- Be aware of content, contact and conduct risks
- Embed online safety within curriculum delivery
- Recognise indicators of exploitation, grooming or radicalisation
- Escalate concerns immediately to the DSL
- Record incidents on the safeguarding system
- Never investigate safeguarding matters independently

4. Filtering & Monitoring

The Provision:

- Uses filtered and monitored internet access
- Reviews filtering regularly
- Monitors network activity proportionately

Staff must:

- Not attempt to bypass filtering
- Report any filtering concerns immediately
- Understand that monitoring may identify safeguarding risks

Filtering alone is not sufficient; supervision and professional judgement remain essential.

5. Use of Devices and Digital Platforms

All technology used within Compass Learning & Education must support safeguarding, data protection and professional conduct. The use of devices is a regulated activity and subject to monitoring.

5.1 Authorised Devices

Staff must:

- Use only provision-issued or formally authorised devices for any communication with students, parents or external professionals
- Never use personal devices, personal email accounts or personal social media platforms for communication with students
- Ensure that all communication regarding students, staff or HR matters takes place through approved internal systems only
- Any exception must be formally authorised by the Head of Provision and recorded.

5.2 Device Security

- Staff are responsible for ensuring that all devices used for work purposes are secure at all times.
- Staff must:
- Lock devices immediately when unattended
- Use strong passwords in line with provision policy
- Enable two-factor authentication where available
- Ensure devices automatically lock after inactivity
- Store devices securely when off-site
- Report lost or stolen devices immediately
- Failure to maintain device security may constitute a data breach.

5.3 Data Handling and Encryption

Staff must:

- Only access personal data that is necessary for their role
- Ensure that any personal or sensitive data stored electronically is encrypted
- Use secure, provision-approved systems for storing and sharing data
- Never download or transfer confidential information onto personal devices or unencrypted storage media
- Double-check recipients before sending emails containing personal data
- Any suspected or actual data breach must be reported immediately to the Data Protection Lead.

5.4 Software and Applications

- Staff must not install, download or use unauthorised software, apps or browser extensions on provision devices.
- Before using any new digital platform, app, website or software with students, staff must ensure that:
- The platform has been approved by the Head of Provision
- Safeguarding risks have been considered
- Privacy settings are checked and configured appropriately
- Chat, messaging or user-generated content functions are risk assessed
- Advertising content does not expose students to inappropriate material
- Age restrictions are compliant with student age
- Free platforms must be treated with particular caution due to embedded advertising and data harvesting risks.

5.5 Approval Process for New Platforms

Before introducing any new digital platform or software, the following must be completed:

- A documented Data Protection Impact Assessment (DPIA), where required
- Confirmation of UK GDPR compliance
- Review of privacy policy and data storage location
- Safeguarding suitability check
- Risk assessment covering misuse, communication functions and data access
- Confirmation of appropriate licensing
- No new platform may be used with students until written approval has been granted by the Head of Provision.

5.6 Monitoring and Accountability

Staff must be aware that:

- Network activity may be monitored for safeguarding and security purposes
- Internet usage logs may be reviewed
- Misuse of technology may result in disciplinary action

- Serious breaches may be referred to external agencies
- The safe use of technology is a professional responsibility and forms part of safeguarding duties.

6. Publishing Images

Staff must:

- Follow the Image Use Policy
- Ensure parental consent before publishing student images
- Avoid identifying vulnerable students
- Store images securely

7. Email & Communication

Staff must:

- Use professional language at all times
- Avoid emotional or reactive responses
- Check recipients carefully before sending
- Use BCC appropriately
- Avoid chain emails

Sensitive data must be encrypted.

8. Remote Learning

Where remote learning is delivered:

- Approved platforms only
- Camera use must follow safeguarding guidance
- Recording must comply with privacy controls
- Staff must maintain professional presentation and background

9. Cybersecurity & Data Protection

Staff must:

- Comply with UK GDPR & Data Protection Act 2018
- Report data breaches immediately
- Use secure storage systems
- Not remove confidential data from secure systems without authorisation

10. Artificial Intelligence & Emerging Risks

Staff must:

- Ensure AI use complies with academic integrity
- Fact-check AI-generated content
- Not upload personal student data into AI tools
- Teach students about misinformation and deepfake risks

11. Reporting & Escalation

All online safety concerns must be:

- Reported to the DSL immediately
- Recorded on the safeguarding system
- Escalated externally where required

Allegations relating to staff online conduct will be referred to the Head of Provision and, where appropriate, LADO.

Staff Declaration

I have read and understood the E-Safety & Acceptable Use Policy and agree to adhere to its requirements.

Name: _____

Signature: _____

Date: _____

Appendix 1 - Potential Online Safeguarding Risks Facing Students

Staff must be aware that learners within Alternative Provision may be disproportionately vulnerable to online harm due to SEMH needs, previous trauma, reduced supervision outside school hours, or exploitation risk.

Students may be exposed to:

Harmful or Illegal Content

Including pornography, extremist material, self-harm content, pro-eating disorder content, gambling, substance misuse promotion, or violence.

Grooming and Sexual Exploitation

Perpetrators may:

- Masquerade as peers
- Move communication to encrypted platforms
- Request explicit images
- Encourage secrecy
- Build dependency before exploitation

Staff must treat online grooming indicators as safeguarding concerns.

Child Criminal Exploitation (CCE)

Students may be:

- Recruited via social media
- Asked to transport drugs or money
- Coerced into sharing information
- Threatened or blackmailed

Online platforms are increasingly used for recruitment.

Online Radicalisation

Students may encounter:

- Extremist narratives
- Manipulative propaganda
- Ideological grooming
- Conspiracy content

Staff must remain vigilant and escalate concerns in line with Prevent duties.

Cyberbullying

Includes harassment, exclusion, image-based abuse, impersonation or doxxing. This may significantly impact SEMH stability.

Image-Based Abuse & Sextortion

Students may experience:

- Pressure to share explicit images
- Threats to distribute images
- Financial exploitation
- Emotional blackmail

All incidents must be treated proportionately and in line with safeguarding guidance.

Online Gaming Risks

Risks include:

- Voice chat grooming
- In-game purchases exploitation
- Gambling-style mechanics
- Exposure to adult content

Misinformation, Deepfakes & AI Manipulation

Students may struggle to critically evaluate manipulated content. Staff should explicitly teach media literacy.

Staff must:

- Recognise early warning signs
- Record concerns promptly
- Escalate through safeguarding systems
- Avoid informal investigation
- Apply professional curiosity