

## **Labyrinth Education**

### **Online Safety Policy and Procedure**

Date of Issue: April 2025

Next Review Date: April 2026

Distribution: All staff and stakeholders

Owner: Senior Leadership Team

Policy Lead: Head of Education

---

### **Scope**

This policy applies to all members of the Labyrinth Education community, including staff, learners, volunteers, parents/carers, visitors, and external partners, who have access to and interact with digital technology, both within and outside Labyrinth Education sites.

Under the Education and Inspections Act 2006 and the 2011 Education Act, staff have the authority to address online safety incidents that occur off-site but are linked to Labyrinth Education. This policy will be applied in conjunction with our Behaviour Policy and Safeguarding Policy.

---

### **Introduction**

Labyrinth Education is committed to providing a safe, inclusive, and innovative digital learning environment. We recognise the benefits of modern technology in education and strive to equip our learners with digital literacy skills while ensuring their safety online. The objective of this policy is to guide staff, learners, and stakeholders in the responsible use of digital technology.

This policy aligns with the following related policies:

- Safeguarding and Child Protection
  - Prevent
  - Behaviour and Anti-Bullying
  - Digital Citizenship Curriculum
  - Data Protection and Privacy
- 

### **Roles and Responsibilities**

#### **Head of Online Safety (HOS)**

- Approves and oversees the effectiveness of the policy.
- Regularly monitors and assesses online safety incidents.

- Ensures online safety training is embedded in staff development.
- Collaborates with technical support teams and safeguarding leads.

#### **Technical Support Team**

- Ensures the security and integrity of digital infrastructure.
- Implements appropriate filtering and monitoring measures.
- Regularly updates security protocols and policies.

#### **All Staff Members**

- Stay informed on online safety policies and best practices.
- Report any suspected online safety breaches.
- Ensure responsible and professional digital communication.
- Incorporate online safety education into the curriculum.

#### **Safeguarding and Wellbeing Team**

- Responds to online safety concerns and incidents.
- Works with external agencies where necessary.
- Educates learners about online risks and responsible digital behaviour.

#### **Learners**

- Follow the Learner Acceptable Use Agreement, have an understanding of what this means in line with their developmental level.
- Report any concerning online activities to a trusted adult.
- Participate in online safety education programs.

#### **Parents/Carers**

- Engage with Labyrinth Education's online safety initiatives.
- Support learners in responsible digital use at home.
- Report concerns related to online safety.

---

### **Education & Training**

#### **For Learners**

- Online safety education is integrated into the curriculum.
- Age-appropriate discussions on cyberbullying, privacy, and digital footprints.
- Encouragement to develop critical thinking about online content.

#### **For Parents/Carers**

- Workshops, newsletters, and online resources.
- Guidance on setting up parental controls and fostering open discussions.

#### **For Staff**

- Regular training sessions on online safety policies and incident response.
  - Updates on emerging online threats and trends.
  - All Labyrinth Education Staff have additional duties under the Counter Terrorism and Securities Act 2015 to ensure that learners/ young people are safe from terrorist and extremist material on the internet
- 

#### **Technical Infrastructure and Monitoring**

- Secure network infrastructure with controlled access levels.
  - Regularly updated filtering systems to block inappropriate content.
  - Monitoring of digital activities to detect potential risks.
  - Compliance with data protection regulations.
- 

#### **Use of Mobile and Digital Devices**

- Personal devices must adhere to Labyrinth Education's acceptable use policies.
  - Staff should only use Labyrinth-provided devices for educational activities.
  - Staff and volunteers are allowed to take digital/video images to support educational aims, with recording kept on secure platforms used to support learners progress monitoring and/or relevant Labyrinth Education secure platforms.
  - The use of digital imagery is restricted and requires parental consent.
- 

#### **Data Protection & Privacy**

- Adherence to GDPR and data protection laws.
  - Clear guidelines on the storage, access, and disposal of personal data.
  - Encryption and secure handling of sensitive information.
- 

#### **Social Media & Digital Communications**

- Staff should use official channels for communication with learners and parents.
- Social media interactions should be professional and in line with ethical guidelines.
- Reporting mechanisms for inappropriate digital content and interactions.

---

## Responding to Incidents of Misuse

- **Low-Level Concerns:** Addressed through education and guidance.
- **Serious Incidents:** Investigated by the safeguarding team, with external agency involvement if necessary.
- **Illegal Activities:** Reported to relevant authorities following established protocols.

---

## Monitoring & Compliance

- Regular policy reviews to adapt to new technological challenges.
- Incident logs to inform policy development.
- Internal and external audits of digital safety measures.

---

## Conclusion

Labyrinth Education prioritises a proactive and preventative approach to online safety. By fostering a culture of digital responsibility, we aim to empower our learners and staff to navigate the online world safely and effectively.

---

## Links to Online Safety Resources and Organisations

The following resources support the development and review of online safety policies and practices at Labyrinth Education:

### Key Online Safety Organisations

- **UK Safer Internet Centre**
- **Childnet**
- **Revenge Porn Helpline**
- **Internet Watch Foundation**
- **Report Harmful Content**

### Professional Standards and Staff Training

- **DfE – Keeping Children Safe in Education**
- **DfE – Safer Working Practice for Adults in Schools**

### Curriculum Support

- **UKCCIS – Education for a Connected World Framework**
- **Teach Today**

### **Bullying, Online Harassment, and Sexting**

- **DfE Cyberbullying Guidance**
- **Anti-Bullying Network**
- **Ditch the Label – Online Bullying Charity**
- **Diana Award – Anti-Bullying Campaign**

### **Prevent and Cybersecurity**

- **Prevent Duty Guidance**
- **NCA – Cyber Prevent**

### **Social Networking and Digital Citizenship**

- **UKSIC – Safety Features on Social Networks**

### **Data Protection and Privacy**

- **360Data – Data Protection Self-Review Tool**
- **ICO – Guides for Education**
- **DfE – Cloud Software and Data Protection Advice**
- **IRMS – Records Management Toolkit for Schools**
- **NHS – Caldicott Principles**
- **ICO – Guidance on Taking Photos in Schools**

### **Parent and Carer Support**

- **Childnet – Parent and Carer Pages**
- **Get Safe Online – Parent Resources**
- **Teach Today – Parent Workshops**
- **Internet Matters**

**Further links and additional resources can be found in the UKCIS Education for a Connected World Framework.**

### **Appendices**

- **Learner Acceptable Use Agreement**
- **Parent/Carer Acceptable Use Agreement**
- **Staff & Volunteer Digital Use Policy**
- **Prevent Policy**
- **Incident Reporting Procedures**

- Technical Security Guidelines