



## **Online Safety Policy**

### **1. Policy Statement**

This policy sets out our commitment to ensuring that learners, Rootz staff, and stakeholders use digital technologies safely and responsibly. As an Alternative Education Provider, we recognise that digital skills are vital for learning and future success - but must be taught and supported in a way that safeguards users from harm.

At Rootz we are committed to promoting a culture of online safety that empowers learners to make informed and safe decisions in the digital world.

### **2. Purpose**

This policy aims to:

- Protect learners from risks associated with online activities.
- Support Rootz staff in providing safe online teaching and guidance.
- Define acceptable use of internet-enabled devices and platforms.
- Prevent incidents of online bullying, exploitation, or access to harmful content.
- Ensure Rootz staff and learners understand their roles and responsibilities regarding digital safety.

### **3. Scope**

This policy applies to:

- All Rootz staff, learners, volunteers, and visitors.
- All digital devices and internet access within the provider's settings.
- Online platforms, websites, and virtual learning environments used for educational purposes.
- Remote learning, communications, and any online interaction involving learners.

#### **4. Roles and Responsibilities**

##### **Designated Safeguarding Lead (DSL)**

- Leads on online safety and keeps up to date with emerging risks.
- Ensures training is delivered and that incidents are managed appropriately.

##### **Rootz Staff**

- Model appropriate online behaviour.
- Educate learners about safe and responsible use of technology.
- Monitor and report any concerns relating to online safety.

##### **Learners**

- Use digital devices and internet services responsibly.
- Report any online concerns, threats, or inappropriate content to a member of staff.
- Follow the Acceptable Use Agreement at all times.

#### **5. Online Safety Education**

Rootz integrate online safety into the curriculum through:

- PHSE and digital literacy lessons.
- Discussions on cyberbullying, consent, privacy, and healthy digital relationships.
- Encouraging critical thinking about online content and social media.
- Promoting the use of safe, educational websites and tools.

#### **6. Acceptable Use**

All users must:

- Use the internet and digital devices only for educational purposes or approved communication.

- Avoid accessing, creating, or sharing harmful, illegal, or inappropriate content.
- Not share personal information online unless with trusted adults and for approved reasons.
- Never engage in or tolerate cyberbullying, harassment, or online abuse.
- Respect privacy, copyright, and intellectual property.

An **Acceptable Use Agreement** must be signed by staff and learners, outlining these responsibilities.

## **7. Managing Risk and Responding to Incidents**

Rootz will respond to online safety concerns by:

- Recording and investigating all reported incidents.
- Referring safeguarding concerns to the DSL.
- Working with external agencies (e.g., police, CEOP) when needed.
- Supporting affected learners with appropriate interventions.
- Implementing disciplinary actions in line with our Behaviour and Safeguarding Policies.

## **8. Use of Social Media and Mobile Devices**

- Rootz Staff must not engage in private online communication with learners.
- Learners should use social media respectfully and with privacy settings enabled.
- Mobile phones should be used in line with the setting's rules (e.g., turned off during sessions).
- Rootz Staff are expected to model appropriate use of personal and professional digital accounts.

## **9. Remote and Online Learning**

When delivering online learning:

- Platforms used must be secure and approved.
- Live sessions must follow safeguarding protocols (e.g., two staff present, no 1:1 video unless pre-approved).
- Recordings may be made for safety and quality assurance.
- Rootz Staff and learners should be dressed appropriately and maintain a professional setting during video calls.

## **10. Monitoring and Filtering**

Rootz use systems that:

- Monitor and log internet use where applicable.
- Block access to inappropriate websites.
- Raise alerts for keywords or behaviours that could indicate a safeguarding risk.

## **11. Training and Awareness**

- Rootz Staff receive regular training on online safety and emerging risks.
- Learners are taught how to protect themselves online through a curriculum approach.
- Parents/carers are supported with resources to reinforce online safety at home.

## **12. Policy Review**

This policy will be:

- Reviewed annually or after significant incidents.
- Updated in line with guidance from DfE, CEOP, NSPCC, and local safeguarding partners.

|                |                       |
|----------------|-----------------------|
| VERSION:       | 0.1                   |
| DATE:          | 23.04.2025            |
| AUTHOR:        | Claire Saunders-Dewes |
| RATIONALE<br>: | Second draft          |
| APPROVED<br>:  |                       |