Tree of Life Educational and
Therapeutic Input Ltd

IT Safety Policy

Tree of Life Educational and Therapeutic Input Ltd

1. Purpose

The purpose of this policy is to ensure the safe, responsible, and appropriate use of information technology, digital devices, and online resources within the Alternative Provision. It aims to:

- Safeguard children and young people from online risks.
- Protect staff from allegations and inappropriate contact.
- Ensure compliance with statutory safeguarding duties (e.g., Keeping Children Safe in Education, Prevent Duty).
- Promote digital literacy and positive online behaviour.

2. Scope

This policy applies to:

- All learners attending the Alternative Provision.
- All staff, contractors, and volunteers.
- All devices and networks provided by the AP, as well as personal devices used on-site or for AP-related purposes.

3. Roles and Responsibilities

Senior Leadership

- Ensure filtering, monitoring, and safeguarding systems are in place.
- Review and update the policy annually.

Staff

- Model safe and professional use of IT.
- Report online safety concerns to the Designated Safeguarding Lead (DSL).

- Use AP-approved communication platforms only.

Learners
- Use technology responsibly and respectfully.
- Report inappropriate content, cyberbullying, or concerns to staff.
- Follow the Acceptable Use Agreement.

Parents/Carers
- Support the AP's IT safety approach.
- Encourage safe use of technology at home.

4. Safe Use of Technology

- Internet Access: Age-appropriate filtering and monitoring systems are in place.
- Devices: Learners may only use AP devices or approved personal devices.
- Social Media: Learners must not contact staff via personal social media accounts. Staff must not engage with learners on personal accounts.
- Recording and Images: No images, videos, or recordings of learners may be made or shared without consent and a clear educational purpose.
- Data Protection: Personal data must be stored securely in line with GDPR.

5. Mobile Phone and Personal Device Safety

Learners
- Mobile phones and personal devices must be handed in at the start of the day (unless specific arrangements are agreed with staff for learning or wellbeing reasons).
- Devices may only be used under staff supervision for an agreed educational purpose.
- The use of phones to record, photograph, or film on site is strictly prohibited.
- Any inappropriate use (e.g., bullying, sharing explicit material, contacting unsafe individuals) will be treated as a safeguarding concern and managed under the Behaviour Policy.

Staff
- Staff must not use personal phones to contact learners. All communication must go through AP-approved channels.
- Personal devices should not be used to take images or store information about learners.
- Mobile phones must be stored securely and not used in teaching spaces unless in an emergency or authorised situation.

Parents/Carers
- Parents are asked to contact the AP through the office rather than via a learner's mobile phone during the day.
- Learners are discouraged from bringing expensive devices to the AP to avoid loss or

theft.

Safeguarding
- Any incidents of sexting, online grooming, or inappropriate sharing will be referred to the DSL immediately.
- Confiscated devices will be managed in line with DfE guidance and safeguarding procedures.

6. Online Risks and Safeguarding

- Cyberbullying: Any incidents will be dealt with under the AP's Behaviour Policy.
- Inappropriate Content: Access attempts will be logged and investigated.
- Radicalisation/Extremism: Concerns will be referred under the Prevent Duty.
- Sexual Harassment/Online Abuse: Reported in line with safeguarding procedures.

7. Training and Education

- Staff receive annual training on online safety and safeguarding.
- Learners receive digital literacy and online safety education as part of their curriculum.

8. Incident Reporting

- Concerns must be reported immediately to the DSL – Tracy Chapman-Ward
- The AP maintains records of online incidents.
- Serious incidents may be referred to external agencies (e.g., police, LADO, CEOP).

9. Monitoring and Review

- The IT systems are regularly monitored for misuse.
- This policy is reviewed annually and after any significant incidents or changes in legislation.

10. Linked Policies

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection Policy
- Staff Code of Conduct