Target English International

Online safety policy

1. Purpose & Scope

This Online Safety Policy sets out how Target English International will help learners, staff, and partners use digital technology safely, especially those aged **10–18**. It covers online behaviour, teaching practices, safeguarding duties, and legal responsibilities.

The policy applies to:

- Learners aged **10–18**
- Managers, Teachers, Activity Leaders and administrative staff
- Contractors, and partners
- Use of school devices, networks, learning platforms, and personal devices when used for school activities

This policy forms part of our **safeguarding and child protection framework** and supports compliance with British Council UK Accreditation criteria for safety and wellbeing.

2. Core Principles

TEI approach to online safety:

- **Safeguarding first** — protecting young people from harm online.
- **Education and empowerment** — teaching safe and responsible online behaviour.
- **Personal data protection** — complying with UK GDPR and relevant children's data protection standards.
- **Legal compliance** — following UK law on online safety and digital harms.

3. Legal & Regulatory Framework

Target English International adheres to the following UK laws and guidance:

3.1 Online Safety Act (UK)

The Online Safety Act requires online platforms to prevent children accessing harmful content (e.g., pornography, self-harm, violence) and enforce age checks. It places duties on tech firms and reinforces safe reporting and moderation mechanisms.

3.2 Teaching Online Safety Guidance

Non-statutory guidance for teaching online safety is sourced through British Council and UK government resources and is aligned with computing, relationships, and health education. We adopt the British Council's safeguarding approach to empower learners and protect them from harm.

4. Definitions

Harmful content — any material that may cause physical, emotional, or psychological harm (e.g., violence, exploitation, self-harm guides).
Personal data — information which identifies a person (e.g., email, name, identity details).
Safeguarding — measures to protect the health and wellbeing of individuals, especially children.

5. Governance, Roles & Responsibilities

5.1 TEI Online Safety

The DSL shall:

- Oversee this policy implementation.
- Coordinate training and incident response.

5.2 Staff Responsibilities

All staff must:

- Model safe online behaviours.
- Report concerns via safeguarding channels.
- Integrate online safety into their teaching.

5.3 Staff and Students

TEI staff and students must:

- Engage respectfully and safely online.
- Use TEI digital tools only for appropriate educational purposes.
- Report concerns to the DSL and/or Senior staff member.

6. Safe Use of Technology

6.1 Acceptable Use

Students/TEI staff must not:

- Share private information online.
- Access illegal or age-inappropriate content.

Students/Staff must:

- Use any necessary school-approved platforms responsibly.
- Keep passwords private.
- Report harmful or uncomfortable material immediately.

6.2 Filtering & Monitoring

Appropriate filters and monitoring tools are in place to reduce exposure to inappropriate content on campus networks and devices (TBC)

6.3 Use of Personal Devices

Bring Your Own Device (BYOD) is permitted and must comply with TEI and Host venue guidelines.

7. Education & Guidance for Ages 10–18

Teaching online safety should be **developmentally tailored**. Educators should:

7.1 10–12 Year-Olds

Focus on:

- Fundamental concepts: digital footprints, privacy settings.
- Safe communication: strangers, friend requests.
- Reporting concerns to trusted adults.

Example conversation prompts:

- "Can you show me how you check privacy settings on this app?"
- "Who do you talk to if something online makes you uncomfortable?"

7.2 13–15 Year-Olds

Focus on:

- Recognising persuasive design, misinformation.
- Balanced screen time and wellbeing.
- Digital citizenship and respectful interaction.

Example guidance:

- "What makes a responsible digital citizen?"
- "How do you decide what to post?"

7.3 16–18 Year-Olds

Focus on:

- Critical media literacy and consent online.
- Risks around sexting, data sharing, exploitation.
- Legal awareness (e.g., laws against sharing intimate images).

Example discussion:

- "What would you do if a friend asked for an explicit image?"
- "Who do you trust to help if something goes wrong online?"

Target English International

Teaching Resources

Use of UK government teaching frameworks click here for gov.uk teaching resource and British Council materials designed for school age groups. Click here for British Council teaching resource

https://learnenglishteens.britishcouncil.org/study-break/magazine-zone/online-safety-uk

8. Responding to Incidents

If a learner experiences or reports an online safety issue:

1. **Record the concern** using TEI safeguarding procedures.
2. **Assess risk** and intervene immediately if safety is at risk.
3. **Support the learner** with guidance, referrals, and/or parental contact.
4. **Escalate to police/children's services** if there is evidence of criminal behaviour.

9. Parental Engagement

Parents/carers (TEI Staff) should be:

- Informed about online risks and school strategies.
- Provided with practical guidance on supervision and controls.
- Encouraged to discuss online experiences openly with children in their care.

You can share this British Council *five golden online safety rules* with families.
https://www.teachingenglish.org.uk/sites/teacheng/files/StaySafe%20A4.pdf

10. Monitoring, Review & Continuous Improvement

This policy will be reviewed annually and updated based on:

- New legislation (e.g., Ofcom codes, Online Safety Act implementation).
- Risk assessments.
- Feedback from staff, learners, and parents.
- Audit of any incidents and training uptake.
- British Council Accreditation criteria
- YLEUK and English UK training and guidance provision

Review due – Jan 2027