

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)



Learner Online Safety Policy

1. Purpose of this Policy

TOAST is committed to promoting a safe, inclusive and supportive learning environment where learners are able to access digital technologies confidently and responsibly.

Technology plays an important role in education, communication, independence and preparing learners for adulthood. Whilst digital technologies provide many opportunities, they also present risks that may place children and young people at risk of harm.

This policy outlines how TOAST promotes online safety, protects learners from online risks and supports staff to respond appropriately to online safeguarding concerns.

Online safety is recognised as an integral part of safeguarding and should be considered in all aspects of teaching, learning and learner support.

This policy has been developed with reference to the Department for Education's **Keeping Children Safe in Education (KCSIE) - Current Version** and reflects the expectation that online safety is an integral part of safeguarding. TOAST will ensure that online safety is embedded throughout safeguarding practice, curriculum delivery and organisational culture in accordance with current statutory guidance.

2. Links to Other Policies

This policy should be read alongside the following:

- Safeguarding Children and Young People Policy
- Child-on-Child Abuse Policy
- Data Protection and Confidentiality Policy
- Acceptable Use of Technology Policy
- Staff Code of Conduct
- Positive Behaviour Support Policy
- Equality, Diversity and Inclusion Policy
- Learner Voice and Co Design Policy
- Compliments, Complaints and Feedback Policy
- Work Experience and Employer Engagement Policy

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)



Statutory Guidance

This policy has been developed in accordance with:

- Keeping Children Safe in Education (KCSIE) - Current Version
- Working Together to Safeguard Children
- Teaching Online Safety in Schools (Department for Education)
- UK Council for Internet Safety (UKCIS) - Education for a Connected World Framework
- Prevent Duty Guidance

3. Associated Procedures

The following procedures support this policy:

- Safeguarding Reporting Procedure
- Recording Concerns Procedure
- Behaviour Incident Procedure
- Risk Assessment Procedure
- Mobile Device Procedure
- Social Media Guidance
- Information Sharing Procedure

4. Principles

TOAST believes that:

- Online safety is everyone's responsibility.
- Every learner has the right to access technology safely.
- Learners should be supported to become confident and responsible digital citizens.
- Staff should model safe and appropriate online behaviour.
- Online safeguarding concerns must be treated as safeguarding concerns.
- Learners should be encouraged to seek help if something online makes them feel worried, unsafe or uncomfortable.
- Online safety education should be embedded throughout learning programmes in accordance with Keeping Children Safe in Education (KCSIE).

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)



5. Scope

This policy applies to:

- All learners.
- All staff.
- Volunteers.
- Contractors.
- Visitors using TOAST digital equipment or networks.
- Learning activities both on and off site where technology is used.
- Work experience placements where digital technology forms part of the placement.

The policy covers the use of:

- Computers.
- Laptops.
- Tablets.
- Mobile phones.
- Interactive displays.
- Social media.
- Email.
- Messaging platforms.
- Educational software.
- Artificial Intelligence (AI) tools where appropriate.

6. Online Risks

In line with **Keeping Children Safe in Education (KCSIE)**, TOAST recognises four broad categories of online risk, commonly known as the **4Cs Framework**. These categories provide the basis for online safety education, risk assessment and safeguarding practice.

Content Risks

Learners accessing harmful, illegal or inappropriate content.

Examples include:

- Violent material.
- Extremist content.
- Pornographic material.
- Self-harm content.

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durrant (Quality and Compliance Manager)

- Misinformation.

Contact Risks

Learners communicating with individuals who may present a risk.

Examples include:

- Online grooming.
- Exploitation.
- Fraud.
- Radicalisation.
- Coercion.

Conduct Risks

Unsafe behaviour online.

Examples include:

- Cyber bullying.
- Sharing inappropriate images.
- Harassment.
- Online abuse.
- Hate speech.
- Sharing personal information.

Commercial Risks

Learners may be exposed to:

- Online scams.
- Fraud.
- In-app purchases.
- Gambling.
- Financial exploitation.
- Misleading advertising.

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)



7. Teaching Online Safety

Online safety is embedded throughout the learner journey.

In accordance with **Keeping Children Safe in Education (KCSIE)**, online safety is not taught as a standalone topic but is embedded throughout teaching, learning, safeguarding and learner support. Learners will be supported to develop the knowledge, skills and resilience required to recognise online risks, make informed decisions and seek help when required.

Learners will be supported to understand:

- Safe internet use.
- Protecting personal information.
- Creating strong passwords.
- Privacy settings.
- Safe use of social media.
- Healthy online relationships.
- Consent.
- Recognising scams.
- Cyber bullying.
- Reporting concerns.
- Artificial Intelligence and responsible use.
- Digital footprints.

Teaching will be adapted to meet individual learner needs using accessible communication methods where appropriate.

8. Staff Responsibilities

All staff are responsible for:

- Modelling safe online behaviour.
- Following organisational ICT procedures.
- Promoting online safety during learning.
- Supervising learners appropriately.
- Reporting online safeguarding concerns immediately.
- Maintaining professional boundaries online.
- Protecting confidential information.
- Using organisational devices responsibly.
- Understanding the online safeguarding risks identified within Keeping Children Safe in Education (KCSIE).
- Maintaining up-to-date knowledge of emerging technologies and online risks.

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)

- Completing safeguarding and online safety training.
- Promoting the safe and ethical use of Artificial Intelligence (AI).



Staff must never communicate with learners through personal social media accounts or unauthorised messaging applications.

9. Learner Responsibilities

Learners are expected to:

- Use technology respectfully.
- Keep passwords private.
- Report anything online that makes them feel unsafe.
- Respect the privacy of others.
- Use devices appropriately.
- Follow staff instructions.
- Treat others kindly online.
- Not share inappropriate images or information.
- Respect copyright and intellectual property.

Support will be provided where learners require assistance to understand these expectations.

10. Use of Artificial Intelligence (AI)

TOAST recognises that Artificial Intelligence (AI) is becoming increasingly common in education and employment.

Learners may use approved AI tools to support learning where authorised by staff.

AI should:

- Support learning rather than replace it.
- Be used ethically.
- Not be used to produce work dishonestly.
- Not be used to generate harmful or inappropriate content.
- Never replace professional judgement.

Staff will support learners to understand both the opportunities and limitations of AI technologies.

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)



11. Cyber Bullying

Cyber bullying is recognised as a form of child-on-child abuse and will be managed as a safeguarding concern where appropriate.

Cyber bullying may include:

- Threatening messages.
- Repeated unwanted contact.
- Sharing rumours.
- Posting offensive comments.
- Image-based abuse.
- Excluding individuals from online groups.
- Impersonation.

Any concerns should be reported immediately to the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead.

12. Reporting Online Safety Concerns

Any online safety concern should be treated seriously.

In accordance with **Keeping Children Safe in Education (KCSIE)**, online incidents will be managed using the same safeguarding principles as offline concerns. Staff should consider whether an online incident indicates wider safeguarding concerns requiring additional intervention or referral.

Staff must:

- Ensure the learner is safe.
- Reassure the learner.
- Avoid deleting evidence where possible.
- Record the concern factually.
- Inform the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead immediately.
- Record the concern on the Zoho Young People Hub.

Where criminal activity is suspected, appropriate external agencies, including the Police, may be contacted.

Staff should never investigate online safeguarding concerns themselves.

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)



13. Parents, Carers and Partnership Working

TOAST values the role of parents, carers and partner agencies in promoting online safety.

Where appropriate, TOAST will:

- Share online safety guidance.
- Signpost families to trusted resources.
- Communicate concerns appropriately.
- Work collaboratively with external professionals.
- Promote consistent online safety messages.

14. Equality and Inclusion

TOAST recognises that learners with Special Educational Needs and Disabilities (SEND) may experience additional online risks or require additional support to understand online safety.

Reasonable adjustments will be made to ensure online safety education is accessible to all learners through:

- Visual resources.
- Easy Read materials.
- Alternative communication methods.
- Practical learning activities.
- Repetition and reinforcement.
- Person centred approaches.

15. Confidentiality

Online safety concerns will be managed in accordance with safeguarding legislation, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and Keeping Children Safe in Education (KCSIE).

Information will only be shared with those who have a legitimate professional need to know.

Where safeguarding concerns exist, confidentiality cannot be guaranteed.

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)



16. Quality Assurance

The effectiveness of this policy will be monitored through:

- Safeguarding audits.
- Incident monitoring.
- Zoho Young People Hub record audits.
- Learner feedback.
- Staff supervision.
- Observation of Teaching, Learning and Assessment (OTLA).
- Internal Quality Assurance (IQA).
- Annual review against the latest edition of Keeping Children Safe in Education (KCSIE).
- Annual policy review.

Learning from incidents and emerging online risks will be used to strengthen online safety practice.

17. Monitoring and Review of this Policy

This policy will be reviewed annually or sooner where required following:

- Publication of a new edition of Keeping Children Safe in Education (KCSIE).
- Changes in legislation.
- Updates to statutory safeguarding guidance.
- Technological developments.
- Emerging online risks.
- Ofsted inspection findings.
- Learning from incidents.
- Organisational changes.

The Leadership Team will ensure the policy remains effective, current and reflects best practice in online safety.

Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)



Appendix 1 - Guidance for Learners

Remember the SMART Rules:

- **Safe** - Keep your personal information private.
- **Meet** - Never meet someone you only know online without a trusted adult.
- **Accept** - Don't accept files, links or friend requests from people you don't know.
- **Reliable** - Not everything online is true. Check information with a trusted adult or member of staff.
- **Tell** - Tell a member of staff or trusted adult if something online makes you feel worried, upset or unsafe.

If you're unsure, stop, don't respond, and ask for help!

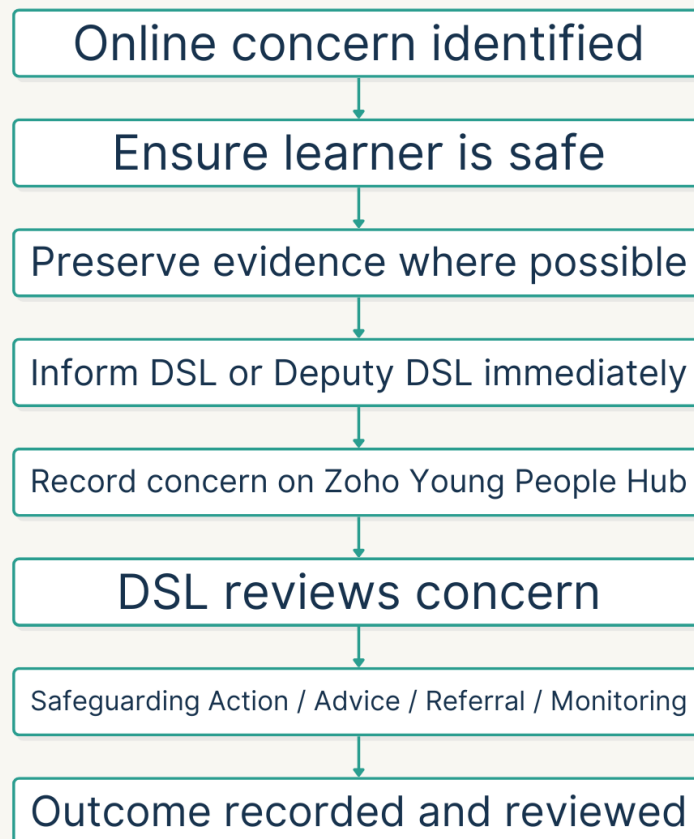
Issue Date: *August 2026*

Review Date: *July 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)

Appendix 2 – Reporting Flowchart

Online concern identified



Issue Date: August 2026

Review Date: July 2027

Lead Officer: Roxy Durran (Quality and Compliance Manager)



Appendix 3 - Legislative and Statutory Framework

This policy has been developed with reference to the following legislation and statutory guidance:

- Keeping Children Safe in Education (KCSIE) – Department for Education (Current Version)
- Working Together to Safeguard Children
- Teaching Online Safety in Schools – Department for Education
- UK Council for Internet Safety (UKCIS) – Education for a Connected World Framework
- Prevent Duty Guidance
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Children Act 1989
- Children Act 2004

Policy Review Record.

Date	Notes	Name	Role	Sign
July 2026	Policy Created	Roxy Durran	Quality and Compliance Manager	
24/08/2026	Policy implemented	Roxy Durran	Quality and Compliance Manager	