

E-SAFETY (ONLINE SAFETY) POLICY

Bury Tuition Centre

Part of North West Education Hub Ltd

1. Introduction

Bury Tuition Centre recognises that technology is an important part of education and everyday life. Online resources, digital platforms and emerging technologies can support learning, communication and development, but they can also expose children and young people to harm.

We are committed to helping students use technology safely, responsibly and respectfully and to ensuring that staff understand how to identify, respond to and escalate online safety concerns.

This policy forms part of the Centre's wider safeguarding framework. It has been reviewed with regard to current national safeguarding and online-safety guidance, including Keeping Children Safe in Education (KCSIE).

2. Scope

This policy applies to students, parents/guardians, staff, tutors, volunteers and other adults working on behalf of Bury Tuition Centre. It covers:

- use of Centre-owned or Centre-managed devices, networks and online services;
- personal devices used on Centre premises or in connection with tuition;
- online tuition and digital communication connected with the Centre;
- online behaviour outside the Centre where it affects the safety, welfare or learning environment of a student or member of the Centre community.

3. Understanding Online Safety Risks

Online safety risks can arise through four broad areas:

Content: being exposed to illegal, inappropriate or harmful material, including violent, sexual, extremist, discriminatory, self-harm or other age-inappropriate content, misinformation or harmful AI-generated content.

Contact: harmful interaction with other people online, including grooming, exploitation, coercion, scams, impersonation or unwanted contact.

Conduct: a person's own online behaviour or the behaviour of others towards them, including cyberbullying, harassment, sharing images without consent, sexual harassment, threatening behaviour or misuse of personal information.

Commerce: risks arising from online advertising, fraud, scams, gambling-like features, financial exploitation or other harmful commercial activity.

4. Our Commitment

Bury Tuition Centre will take reasonable steps to:

- promote safe, respectful and responsible use of technology;
- protect students from online harm and respond appropriately when concerns arise;
- ensure staff understand their safeguarding responsibilities in relation to online safety;
- use appropriate, secure and access-controlled systems for enrolment, administration and communication;
- apply suitable filtering, supervision and/or monitoring arrangements to Centre-managed internet access and devices, proportionate to how technology is used at the Centre;
- review online-safety risks when new technology, services or working practices are introduced, including generative artificial intelligence (AI);
- support parents/guardians with online-safety concerns where appropriate.

The Centre no longer uses TutorBird as its student-management platform. Online safety and data protection requirements apply regardless of which approved systems or service providers the Centre uses.

5. Expectations for Students

Students are expected to:

- use technology, internet access and digital resources responsibly and in accordance with staff instructions;
- treat others respectfully in online and digital interactions;
- never use technology to bully, intimidate, threaten, discriminate against or harass another person;
- keep passwords and personal information private and not attempt to access another person's account;
- not attempt to bypass security, filtering or access restrictions, including through unauthorised VPNs, proxies or similar methods;
- not deliberately access, create, save or share illegal, harmful or inappropriate content;
- not take, make or share photographs, videos, audio recordings or screenshots of another person without appropriate permission;
- not use generative AI or other digital tools to create deceptive, abusive, sexualised, discriminatory or harmful content about another person;
- tell a trusted adult or member of staff if something online makes them feel unsafe, uncomfortable, pressured or worried.

6. Personal Devices and Mobile Phones

Personal devices may only be used during tuition where permitted by the tutor or Centre and for an appropriate purpose.

- Students must follow staff instructions about when phones, tablets, smartwatches or other devices should be put away.
- Students must not photograph, film or record staff or other students without permission.
- Personal devices must not be used to access or share inappropriate content on Centre premises.
- Where misuse creates a safeguarding, safety or behaviour concern, the matter will be managed under the Centre's safeguarding and Behaviour & Code of Conduct procedures.

7. Expectations for Parents / Guardians

Parents and guardians play an important role in supporting children's online safety. We encourage parents/guardians to:

- have regular, age-appropriate conversations with their child about safe and respectful use of technology;
- support reasonable boundaries for device, social-media, gaming and internet use;
- use security settings and parental controls where appropriate;
- encourage their child to report concerning online contact or content without fear of being blamed;
- tell the Centre promptly about an online-safety issue that may affect their child's safety, wellbeing or participation at Bury Tuition Centre;
- support the Centre's expectations regarding mobile phones, recordings, cyberbullying and digital behaviour.

8. Expectations for Staff and Tutors

Staff and tutors must maintain professional standards and appropriate boundaries in all use of technology.

- use Centre-approved methods of communication for Centre business wherever required;
- avoid inappropriate private or personal online contact with students;
- not use personal social-media relationships with students in a way that compromises professional boundaries;
- supervise student use of technology during tuition where appropriate;
- follow the Centre's safeguarding, data-protection, photography and behaviour requirements;
- report online-safety or filtering/monitoring concerns promptly through the appropriate route;
- not use personal devices to photograph or record students unless specifically authorised for a legitimate Centre purpose and handled in accordance with Centre policy;
- consider privacy, safeguarding, accuracy, age-appropriateness and data-protection risks before using AI or other emerging technology with students.

Any concern about an adult's online communication or behaviour towards a child must be reported and managed in accordance with the Centre's safeguarding procedures.

9. Online Tuition and Digital Communication

Where online tuition or digital communication is used:

- the Centre will use approved platforms or communication methods;
- staff will maintain the same professional boundaries expected during face-to-face tuition;
- students should participate from an appropriate environment and parents/guardians should be aware of the arrangements for younger students;
- links, meeting details and passwords must not be shared with unauthorised people;
- staff should not communicate with students through disappearing-message functions or other channels that prevent appropriate accountability, unless specifically authorised and risk-assessed;
- any recording of an online session must have a clear, legitimate purpose and must comply with safeguarding, privacy and data-protection requirements.

Online sessions will not be routinely recorded merely because they are online. Where recording is proposed, participants will be informed and the Centre will determine the appropriate lawful basis, access controls and retention arrangements.

10. Filtering, Monitoring and Centre Technology

Where Bury Tuition Centre provides internet access or Centre-managed devices for students, it will take proportionate steps to reduce access to harmful or inappropriate online material without unnecessarily preventing legitimate learning.

- Filtering and monitoring arrangements will reflect the age and needs of students and the way technology is used at the Centre.
- Staff must know how to report concerns where unsuitable material is accessible, filtering appears to have failed or online activity gives rise to a safeguarding concern.
- High-risk concerns should be escalated promptly to the Designated Safeguarding Lead (DSL).
- The Centre will review the effectiveness and appropriateness of its filtering and monitoring arrangements at least annually where such systems are in use, and sooner where a significant risk, system change or new technology requires review.
- No filtering or monitoring system can remove all online risk; supervision, education, professional judgement and clear reporting arrangements remain important.

11. Artificial Intelligence (AI) and Emerging Technology

Generative AI and other emerging technologies can support learning but can also create safeguarding, accuracy, privacy and academic-integrity risks.

- Students must follow tutor instructions about whether and how AI may be used for learning.
- Students must not enter sensitive personal information about themselves or another person into an AI service unless the Centre has specifically approved that use.
- AI-generated information should not automatically be treated as accurate and should be checked appropriately.
- AI must not be used to generate or manipulate sexualised, abusive, discriminatory, threatening, deceptive or humiliating material involving another person.
- Staff must consider safeguarding and data-protection risks before introducing a new AI service or asking students to use one.

12. Cyberbullying, Harmful Content and Image Sharing

Cyberbullying and online harassment are treated as behaviour and safeguarding matters, not simply as technology issues.

The Centre will respond to concerns involving threatening messages, discriminatory abuse, impersonation, sexual harassment, non-consensual image sharing, harmful rumours, deliberate exclusion, coercion or other online behaviour that may cause harm.

Where an incident involves sexual images of a child, suspected grooming, exploitation, criminal behaviour or another serious safeguarding concern, staff must not investigate informally by forwarding, downloading or unnecessarily

viewing harmful material. The concern must be referred promptly to the DSL so that appropriate safeguarding procedures can be followed.

13. Reporting and Responding to Concerns

Students should tell a trusted adult as soon as possible if they experience or witness something online that makes them feel unsafe, uncomfortable, threatened or worried.

Staff must report online-safety safeguarding concerns to the DSL or Deputy DSL promptly. The Centre will:

- listen to the concern and take it seriously;
- record relevant information appropriately;
- consider immediate steps needed to protect the student or others;
- involve parents/guardians where appropriate and safe to do so;
- consider whether information should be shared with a school, local authority, police or another safeguarding agency;
- preserve relevant evidence appropriately without unnecessarily copying or distributing harmful content.

Safeguarding Contacts

Designated Safeguarding Lead (DSL): Shazia Tahir
Email: safeguarding@northwesteducationhub.co.uk
Phone: 07527 675842

Deputy Designated Safeguarding Lead (Deputy DSL): Nazia Younis
Email: info@northwesteducationhub.co.uk
Phone: 07485 184081

14. Misuse of Technology and Consequences

Misuse of technology will be considered in line with the Centre's Behaviour & Code of Conduct Policy and safeguarding procedures.

- Staff may give an instruction, warning or restriction where behaviour is low-level and can be addressed safely.
- Parents/guardians may be contacted and a behaviour-support approach may be agreed where concerns persist.
- Serious or repeated misuse may lead to suspension or removal from the Centre in accordance with the Terms & Conditions and Behaviour & Code of Conduct Policy.
- The Centre does not need to progress through every behaviour stage before taking action where an incident is serious or creates an immediate safeguarding or safety concern.
- Where appropriate, serious incidents may be referred to external agencies.

15. Data Protection and Privacy

Online-safety activity may involve personal information, including safeguarding records, communications, device information or monitoring records. Such information will be handled in accordance with the Centre's Data Protection & Privacy Policy.



Access to sensitive information will be limited to those who need it for their role. Information will be retained only for as long as required by the relevant safeguarding, legal, operational or data-retention requirements.

16. Related Policies

- Safeguarding / Child Protection Policy
- Behaviour & Code of Conduct Policy
- Data Protection & Privacy Policy
- Equality, Anti-Bullying & Complaints Policy
- Photography & Use of Images Policy
- Terms & Conditions

17. Monitoring and Review

This policy will be reviewed at least annually and sooner where required because of a significant safeguarding incident, changes in technology, new systems or services, changes to Centre practice, or updated legislation or national guidance.

The Centre will also review relevant online-safety controls when new technologies, including AI tools, are introduced.

18. Legal Entity

Bury Tuition Centre is a trading name of North West Education Hub Ltd.

Policy Information

Policy Owner	Nazia Younis (Director / Deputy DSL)
Policy Reviewed	August 2026
Next Review Due	August 2027
Version	2.0