Online Safety Policy

Policy status	Non-statutory
Reviewed	24th March 2025
Next review date	October 2025

Safeguarding Statement

At Beatrice Tate School we respect and value all children and young people and are committed to providing a caring, friendly and safe environment for all our students so they can learn, in a relaxed and secure atmosphere. We believe every student should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Beatrice Tate School. We recognise our responsibility to safeguard all who access school and promote the welfare of all our learners by protecting them from physical, sexual and emotional abuse, neglect and bullying.

Online Safety Policy

Contents

Online Safety Policy

Version	Date	Author	Description of change
October 2022	10.10.22	MW/WH	Original E-safety Policy
March 2025	24.03.25	WH/NB	New policy rewrite; renamed Online Safety Policy

Online Safety Policy

1. Introduction

At Beatrice Tate School, we are committed to safeguarding and promoting the welfare of all students, ensuring they learn in a safe and secure environment. This includes protecting them from online risks such as abuse, exploitation, radicalisation, cyberbullying, and exposure to harmful or inappropriate content.

This policy applies to all staff, governors, volunteers, parents, guardians, and students who access school technology, including devices, networks, and online platforms. It sets out expectations for safe and responsible ICT use and outlines measures to identify, prevent, and respond to online safety concerns. The policy also ensures that students with Profound and Multiple Learning Difficulties (PMLD) and Severe Learning Difficulties (SLD) receive tailored safeguarding measures suited to their cognitive and communication needs.

All stakeholders must adhere to the Acceptable Use Agreements (AUA) outlined in the appendices, which provide specific guidance for staff, students, and parents/guardians.

2. Aims

The aims of this policy are to:

- Ensure all students and staff are safeguarded from online harm.
- Provide clear guidelines on acceptable ICT use.
- Outline the school's filtering, monitoring, and incident response procedures.
- Integrate online safety into the curriculum and staff training.
- Establish clear roles and responsibilities for all stakeholders.
- Support students with PMLD and SLD by providing tailored online safety guidance and increased supervision.
- Enhance parental engagement by providing accessible information, training, and support.

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – exposure to illegal, inappropriate, or harmful material (e.g., pornography, fake news, hate speech, radicalisation, extremism, misinformation, AI-generated false content).
- **Contact** – harmful interaction with others (e.g., peer pressure, grooming, exploitation, cyberstalking, identity theft).
- **Conduct** – online behaviours that increase harm (e.g., cyberbullying, explicit image sharing, online fraud, plagiarism, hacking, inappropriate use of social media).
- **Commerce** – risks such as scams, gambling, phishing, and fraudulent transactions.

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE) updated annually, and its advice for schools on:

- Teaching online safety in schools
- Relationships and sex education (RSE)
- Preventing and tackling bullying
- Searching, screening and confiscation

This policy aligns with national statutory guidance, including:

- *UK GDPR and Data Protection Act 2018*
- *The Education Act 2011* (including powers to search students' devices)
- *DfE Filtering and Monitoring Standards (2023)*
- *Prevent Duty Guidance* (on tackling online radicalisation)
- *Children and Social Work Act 2017* (including RSHE requirements)
- *Equality Act 2010* (ensuring accessibility for all students)
- *The Malicious Communications Act 1988* (relevant to cyberbullying and online abuse)
- *The Computer Misuse Act 1990* (regarding hacking, viruses, and unauthorised access)

4. Roles and responsibilities

4.1. The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. Responsibilities include:

- Ensuring online safety is a regular agenda item in safeguarding meetings.
- Overseeing filtering and monitoring systems to ensure effectiveness.
- Ensuring all staff receive annual online safety training as part of safeguarding requirements.
- Reviewing online safety risks and incident logs at least annually.
- Ensuring compliance with national online safety guidelines and statutory safeguarding requirements.

4.2. The Headteacher

The Headteacher is responsible for ensuring that:

- Online safety is embedded into the safeguarding culture of the school.
- The school's filtering and monitoring systems are regularly reviewed for effectiveness.
- All students, staff, and parents are aware of online safety expectations and training opportunities.
- Online safety is prioritised in school development plans and risk assessments.
- There is a clear incident response system in place for online safety concerns.

4.3. The Designated Safeguarding Lead (DSL)

The DSL has overall responsibility for online safety, including:

- **Monitoring and managing online safety incidents**: Ensuring all incidents are logged, investigated, and responded to in line with safeguarding procedures.
- **Providing safeguarding support and intervention**: Working with vulnerable students at higher risk of online harm and offering individualised support.
- **Reviewing filtering and monitoring systems**: Liaising with the ICT Lead to ensure appropriate safeguards are in place.
- **Delivering and organising staff training**: Ensuring all staff understand their responsibilities regarding online safety and providing regular updates.
- **Liaising with external agencies**: Coordinating with the local authority, police, CEOP, and other relevant bodies when required.
- **Leading on online safety curriculum development**: Working with teaching staff to ensure appropriate teaching of digital safety skills.
- **Providing termly reports to governors**: Ensuring they are kept informed of online safety trends, incidents, and policy developments.

4.4. Online Safety Lead

The Online Safety Lead supports the Designated Safeguarding Lead (DSL) by focusing on the educational aspects of online safety. Their key responsibilities include:

- Preparing, organising and delivering staff training sessions on responsible ICT use and online safety risks.
- Keeping up to date with new online threats and best practices, sharing relevant information with staff.
- Helping teachers embed online safety education into the curriculum.
- Advising on age-appropriate digital safety strategies for students with Profound and Multiple Learning Difficulties (PMLD) and Severe Learning Difficulties (SLD).
- Providing accessible guidance and resources to help parents understand online risks and safe digital practices.
- Preparing, organising and delivering parent workshops on internet safety, parental controls and responsible device use.

4.5. ICT Support Officer

The IT Support Officer is responsible for:

- Implementing and maintaining firewalls, filtering, and access controls.
- Conducting weekly system security audits.
- Ensuring software and anti-virus protections are up to date.

- Implementing multi-factor authentication (MFA) for staff where applicable.
- Working with the DSL to address online safety incidents.
- Providing updates to parents on filtering and monitoring measures in place.

4.6. Staff

Staff are responsible for:

- Follow the **Acceptable Use Agreement for Staff** (Appendix 1).
- Supervise students when using digital devices.
- Report online safety concerns **immediately** to the DSL.
- Educate students about safe internet use.
- Model responsible online behaviour and avoid personal use of social media in school settings.
- Differentiate online safety teaching to meet the needs of SEND learners.

4.7. Parents and guardians

- Engage with school-led online safety sessions, newsletters, and updates.
- Use recommended resources (e.g., UK Safer Internet Centre, NSPCC, CEOP).
- Monitor their child's internet activity at home and support safe technology use.
- Attend school-provided training and workshops on online safety.

5. Educating students about online safety

- Online safety will be embedded into the curriculum and adapted to the needs of learners with SLD and PMLD.
- Visual supports, social stories, and sensory-based approaches will be used to reinforce key online safety messages.
- The curriculum will include:
    - Identifying safe and unsafe online behaviours.
    - Understanding digital footprints and privacy.
    - Safe use of assistive technology.
    - Strategies for seeking help if something makes them uncomfortable online.
    - Developing resilience and critical thinking when navigating digital environments.

6. Educating parents/carers about online safety

- The school will provide parents with accessible resources and workshops tailored to their child's needs.

- Parents will be advised on:
    - Implementing parental controls and safe browsing settings.
    - Recognising signs of online risks such as cyberbullying or grooming.
    - Encouraging safe digital habits at home.
    - Managing screen time and digital wellbeing strategies.

7. Acceptable use of the internet in school

- All students, staff and visitors must follow the school's **Acceptable Use Agreements**.
- Access to the internet will be supervised, and assistive technology will be used in a structured manner to support safe digital engagement.
- Staff must ensure that all students understand the rules of internet use through differentiated teaching methods appropriate to their needs.
- The use of personal devices by students and staff must be in line with school policy. Any breach of acceptable use agreements will be addressed in accordance with disciplinary procedures.

8. Filtering and monitoring

- The school employs **LGfL's filtering system** to block harmful content in line with DfE Filtering and Monitoring Standards (2023).
- A **real-time monitoring system** will alert the DSL to potential online risks.
- Staff will regularly review monitoring reports and respond appropriately.
- The IT Support Officer is responsible for overseeing filtering and monitoring systems and ensuring that they are updated to reflect emerging threats.
- The filtering system must not unreasonably impact teaching and learning, and requests for changes to filtering settings must be reviewed and approved by the Headteacher and DSL.

9. Cyberbullying

- Cyberbullying is addressed in the school's **anti-bullying policy** and includes incidents occurring both inside and outside school.
- The school will provide ongoing education on recognising and responding to cyberbullying.
- A clear reporting system will be in place for students, parents, and staff.
- Incidents of cyberbullying will be investigated thoroughly, and disciplinary measures will be applied where necessary.
- Support will be provided to both victims and perpetrators of cyberbullying, including counselling where appropriate.

- The school will collaborate with external agencies, including the police and local authority, when necessary to address severe cases of cyberbullying.

10. Use of AI tools

- Staff must complete a **risk assessment** before using AI tools in lessons.
- The school will educate students on the ethical and safe use of AI.
- AI tools must not be used in a way that facilitates cyberbullying, cheating, or the creation of harmful content.
- Staff must ensure that AI-generated content is age-appropriate and does not expose students to biased or misleading information.
- Any concerns regarding AI misuse must be reported to the DSL immediately.

11. Staff use of work devices outside school

- Work devices must be encrypted and password-protected.
- Personal data must never be stored on personal devices.
- Staff must follow strict protocols when accessing school systems remotely.
- The IT Support Officer will provide guidance on securing devices and data when working remotely.
- Any loss or theft of a work device must be reported immediately to the IT Support Officer and DSL.

12. Responding to online safety incidents

- All concerns must be **immediately reported** to the DSL.
- Cyberbullying, online abuse, and illegal content will be managed under the Behaviour and Safeguarding Policies.
- Parents/carers will be informed of any serious breaches involving their child.
- The school will provide targeted interventions for students who misuse online platforms, including tailored education on digital responsibility.
- Any staff misuse of ICT will be investigated under the **Staff Code of Conduct.**
- If a criminal offence is suspected, the police and/or CEOP (Child Exploitation and Online Protection Agency) will be contacted.
- Data breaches must be reported to the Data Protection Officer (DPO) in line with GDPR.
- Serious incidents will be escalated to the governing body.

13. Training

- Annual online safety training for all staff.

- Ongoing professional development on emerging digital risks.
- Staff will receive specific training on handling online safety incidents and supporting students with SEND in accessing digital learning safely.
- Students will participate in workshops and lessons tailored to their level of understanding to reinforce safe online behaviour.
- Parents/carers will be invited to participate in workshops and provided with resources to support online safety at home.

14. Monitoring and review

- The policy will be reviewed annually by the DSL and IT Support Officer, and approved by the governing body.
- Risk assessments and filtering system reviews will be conducted as part of the review process.
- Immediate updates will be made in response to DfE guidance changes or emerging risks.
- The policy will be shared with parents and guardians to ensure transparency.

15. Links with other policies

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Behaviour Support Policy
- Use of Artificial Intelligence (AI) Policy

16. References and contacts

- **DSL Contact**: Amanda Lambert – deputy@beatricetate.towerhamlets.sch.uk
- **Online Safety Lead**: nblack@beatricetate.towerhamlets.sch.uk
- **IT Support Officer:** it@beatricetate.towerhamlets.sch.uk
- **Data Protection Officer (DPO)**: dpo@beatricetate.towerhamlets.sch.uk
- **NSPCC Helpline**: 0808 800 5000
- **CEOP Reporting:** www.ceop.police.uk

17. Appendix 1: Acceptable Use Agreement for Staff

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of students on a private device. Only school devices should be used to take images for legitimate purposes. • Share confidential information about the school, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Name (staff member/governor/volunteer/visitor):	
Signature:	**Date:**

18. Appendix 3: Acceptable Use Agreement for Students