ONLINE SAFETY POLICY

Approval Date	July 2025
Policy Owner	Head of ICT Services and Infrastructure
Adopted by Trust Board	July 2025
Review Date	December 2026

CONTENTS

Section Page No.

INTRODUCTION

This online safety policy applies to all schools in our Trust. The policy is designed to ensure the safety and well-being of all pupils and staff using technology and the internet. This policy reflects the statutory guidance and best practice for online safety and covers all age ranges from 4 to 18.

This policy should be used in conjunction with Child Protection and Safeguarding Policy, AI Policy, Mobile phone policy and IT acceptable use policies.

RESPONSIBILITIES

The Trust has appointed a Head of Safeguarding who will take the lead on online safety issues. Each school in the Trust will have a designated safeguarding lead who will be responsible for implementing the online safety policy in their school. They will ensure that all staff, pupils, and parents are aware of the online safety policy and the procedures that should be followed in case of online safety concerns.

All staff members have a responsibility to promote online safety and to ensure that pupils are aware of safe online behaviour. Pupils also have a responsibility to follow the online safety policy and report any concerns they may have.

RISK ASSESSMENT

Each school in the Trust will carry out a regular risk assessment of the use of technology in their school to identify any potential risks to pupils and staff. The risk assessment will be reviewed annually and will consider the following:

- The use of school owned mobile devices such as tablets and smartphones
- The use of social media and messaging apps
- Access to inappropriate material
- Cyberbullying
- Online grooming
- Online identity and privacy
- The use of AI technologies in line with the AI policy

PUPILS' USE OF TECHNOLOGY

Pupils will be educated about online safety and will be taught to use technology responsibly, safely and securely. Staff members will monitor pupils' use of technology, and filtering software will be used to block access to inappropriate material.

SOCIAL MEDIA

Pupils are not allowed to access social media platforms during school hours unless it is for educational purposes and approved by a member of staff. Pupils are advised not to share personal information on social media, and staff members will regularly monitor pupils' online behaviour.

MOBILE DEVICES

School Owned Mobile devices such as tablets and smartphones will only be used under the supervision of a member of staff. Pupils are advised not to share their personal information or passwords and to report any concerns immediately.

Pupil owned mobile phones are not to be used within school, details outlined in the Mobile Phone Policy.

CYBERBULLYING

We take cyberbullying very seriously, and all incidents will be dealt with in accordance with our bullying policy. Pupils are advised to report any incidents of cyberbullying immediately.

ONLINE GROOMING

We are committed to protecting our pupils from online grooming. Pupils are advised to be cautious when communicating with people they do not know online and to report any concerns immediately.

ONLINE IDENTITY AND PRIVACY

Pupils are advised to keep their personal information private when using the internet. Staff members will educate pupils about the importance of keeping their personal information secure.

STAFF USE OF TECHNOLOGY

All staff members will be made aware of the online safety policy and their responsibilities regarding online safety. Staff members are advised to use social media responsibly. Staff will be subject to filtering, monitoring and alerting when using School or trust provided devices.

Staff must not contact, follow, or friend, pupils on social media, and must reject any requests from pupils of this nature. Staff must not use instant messaging or chat applications to contact students.

AUTOMATED SAFEGUARDING MONITORING SOLUTIONS

Each school in the Trust will use automated safeguarding monitoring solutions on school devices to help ensure the safety and well-being of pupils when using technology. These solutions are designed to detect and flag any potential risks, such as cyberbullying, online grooming, or access to inappropriate material.

When using these monitoring solutions, we will ensure that pupils are aware that their activity may be monitored, and that any concerns that are identified will be investigated by a member of staff. Pupils will also be informed of the purpose of the monitoring solution and how it will be used to keep them safe.

Staff members will receive training on the use of the monitoring solution and how to respond to any concerns that are identified. A priority system will be used to distribute concerns from the system to ensure that high priority concerns are directed towards the safeguarding team, and other concerns to other members of staff for management. Staff members are expected to review and action in line with agreed timescales.

Designated safeguarding leads will review activities and reports.

Trust wide reporting and analysis will also be undertaken by the safeguarding team.

Changes to monitoring categories or priorities will be managed via a trust-wide approval process.

POLICY HISTORY

Date	Summary of change	Contact	Policy Implementation Date	Review Date
June 2024	Policy implemented	Head of ICT Services and Infrastructure	June 2024	June 2025
June 2025	Risk Assessments: AI technologies will be risk assessed in line with AI policy. Staff use of technology: to make staff aware that the Trust can monitor devices off-site. E-safety references amended to 'online safety'	Head of ICT Services and Infrastructure	July 2025	December 2026