EBOR ACADEMY TRUST

Policy Number

12

E-Safety Policy

Approved By:	Ebor Academy Trust Board of Trustees
Approval Date:	November 2021
Review Period:	Every 3 years
Review Date:	November 2024

Author:	*Tim Moat, Ebor IT Lead*
Date Created/updated:	*August 2021*
Version Number:	*2*

Contents:

1. **Rationale**

Internet use is part of the statutory curriculum and a necessary tool for learning, used to enrich and extend learning activities. Benefits of using the Internet in education include:

a) access to world-wide educational resources including museums and art galleries;
b) inclusion in the National Education Network which connects all UK schools;
c) educational and cultural exchanges between pupils world-wide.

Ebor Academy Trust therefore has a duty to provide pupils with access to safe internet access in order to provide quality learning using internet technologies and electronic communications. With this comes the responsibility to ensure that this learning takes place safely.

ICT has an all-encompassing role within the lives of children and adults. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

a) The Internet
b) E-mail
c) Instant messaging – often using web cams
d) Blogs (an on-line interactive diary)
e) Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
f) Social networking sites
g) Video broadcasting sites
h) Chat Rooms
i) Gaming Sites
j) Music download sites
k) Mobile phones with camera and video functionality
l) Phones with email, web functionality.

The Trust has a responsibility to educate its pupils in the safe use of technologies. This policy recognises our commitment to e-safety and acknowledges its part in the suite of safeguarding practices. It shows our commitment to meeting the requirements to keep pupils safe.

2. Roles in E-Safety

E-Safety depends on effective practice at a number of levels:

a) Responsible ICT use by all staff and pupils
b) Sound implementation of Trust policies, National Education Network standards and specifications, to ensure safe use of technology
c) Curriculum use.
d) The Trust

E-Safety is recognised by the Trust as an essential aspect of strategic leadership.

The Trust sets IT policies and ensures staff, including E-Safety Coordinators, are aware of local and national guidance on e-Safety and are updated at least annually on policy developments.

On joining the Trust, employees are given the Acceptable Use Policy to read and sign as understood. Staff are reminded and updated about e-Safety matters at least once a year and through regular briefings.

2.1. E-Safety Coordinators;

Each school has e-Safety Coordinators;

a) Head of School and Designated Child Protection Coordinator
b) ICT and E-Safety coordinator

They keep up to date with E-Safety issues and guidance through liaison with organisations such as Becta and The 7 Child Exploitation and Online Protection (CEOP)6. They also ensure the Head, staff and Governors are updated as necessary.

2.2. The Headteacher

The Headteacher ensures that the E-Safety, and other associated policies are implemented and compliance monitored and works to embed safe practices into the culture of the school. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

2.3. Teachers

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and complying with IT policies and procedures.
All Trust employees must read, and sign that they have read the Trust's Acceptable Use Policy which includes:

a) Acceptable use of Internet including use of internet-based communication services
b) Acceptable use of school network, equipment and data
c) Acceptable use of digital images and digital technologies, such as mobile phones and digital cameras
d) E-Bullying / Cyberbullying

3. Educating on E-safety

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security; what Internet use is acceptable. Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupil's age and maturity and educate them in the effective use of the Internet, including the skills of knowledge location, retrieval and evaluation.

The teaching of internet safety is included in the ICT Scheme of Work, but all teachers within all year groups should be including Internet safety issues as part of their discussions on the responsible use of the Trusts computer systems. As a minimum pupils will be taught:

a) If they see an unacceptable image on a computer screen, they must lower the screen (laptop) or turn off the screen, and then report immediately to a member of staff.
b) What Internet use is acceptable and what is not and given clear objectives for Internet use.
c) To be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

d) The risk of Online Bullying, how to avoid it and what to do if it happens, during lessons on ICT Safety
e) Not to place personal photos on any social network space.
f) Never to give out personal details of any kind which may identify them or their location
g) The use of social networks brings a range of dangers for children and only moderated social networking sites should be used for a specific age range. Parents will be informed that the minimum age for accessing most well-known sites is 13 (Year 8).

In addition;

h) E-Safety rule Posters will be displayed in classrooms – appropriate to the Key Stage.
i) Pupils will be expected to conform to appropriate standards of behaviour in any forums that may be created.
j) Parents will be informed that pupils will be provided with supervised Internet access.

4. **Use of Email by children**

a) Children may only use approved email accounts on the Trust system.
b) All children's email accounts will be moderated by the class teacher in order to prevent exposure to offensive or inappropriate emails.
c) Children must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
d) Incoming e-mail should not opened unless the author is known
e) Access to external personal email accounts will be allowed for staff only.
f) Email from children to external organisations should be written carefully and authorised before sending, in the same way as a letter written on letter headed paper.
g) The forwarding of chain letters is not permitted.

5. **Use of Social Networking sites by children**

Access to social networking sites and newsgroups in the classroom, by teachers or children, is not allowed.

Additional guidance on staff use of their own personal social media sites is in the Staff Code of Conduct

6. **Use of phones**

a) Mobile phones are not allowed to be used by children whilst in school.
b) Staff will use an Ebor phone where contact with pupils is required.

Additional guidance on staff use of their own personal social media sites is in the Staff Code of Conduct

7. **Use of games**

Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

8. **Published Content and the Academy Website**

a) Staff or pupils' personal information will not be published.
b) The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

9. **Use of still and moving images**

Photographs taken for official school use, which are likely to be stored electronically alongside other personal data are covered by the Data Protection Act.
Before taking or publishing any photographs, video footage etc of pupils, parental permission must be obtained using the Parental Permission Form. This ensures that parents are aware of the way the image of their child is to be used.

10. **Publishing Pupils' Images and Work**

Websites within Ebor will reflect the diversity of activities, individuals and education that can be found throughout the Trust. However, we recognise the potential for abuse that material published on the Internet may attract, no matter how small this risk may be.
Therefore, when considering material for publication on the Internet, the following principles must be followed:

a) Only use images of pupils in suitable dress to reduce the risk of inappropriate use.
b) Consider using group photographs rather than photos of individual children.
c) Pupils' full names will not be used anywhere on the website or learning platform, in association with photographs.
d) No link should be made between an individual and any home address (including simply street names)

11. **Security**

The Trust will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a Trust computer. Neither the Trust nor the school can accept liability for the material accessed, or any consequences of Internet access.

The Trust takes system security very seriously. The measures it follows are detailed in the IT Strategy.

Although this is more difficult with younger children, password policy should add complexity over time and schools must not use generic passwords for children to log in as this increases risk of system breaches.

a) Starting at early years, use 5-8 character passwords that are easy to remember such as colour and animal (for example Reddog, Bluecat, Greenbird) surname and date of birth. For very young children, the teacher may wish to securely retain a list of passwords.

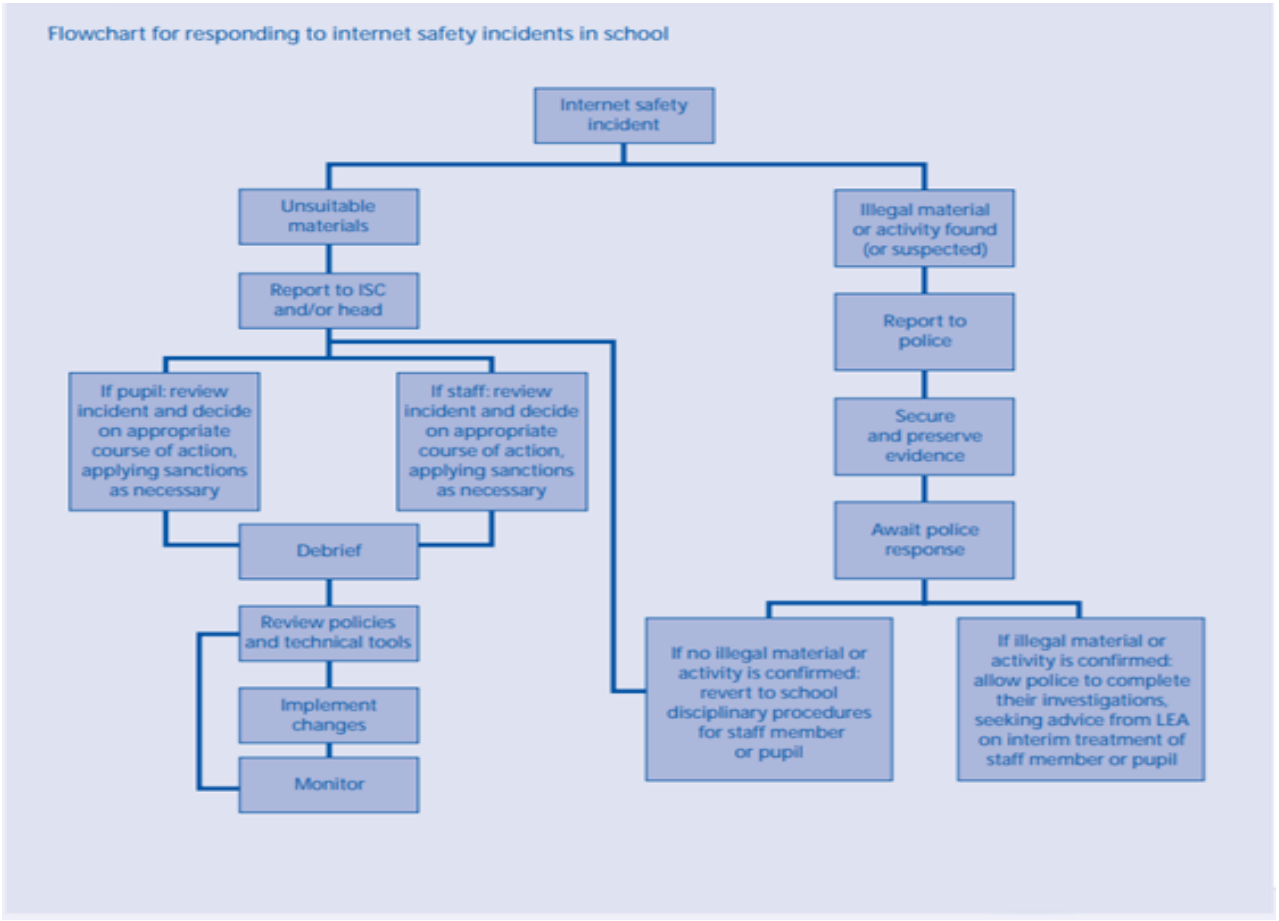
b) As children move through primary, increase the length to 8-12 including letters, numbers and a symbol (for example Reddog21!, Bluecat21@, Greenbird10@).

This approach will also help to educate children about safe use of computers.

12. **Handling e-safety concerns and complaints**

a) Concerns over e-safety should be reported immediately to the E-Safety lead.
b) If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the web filtering provider via the e-safety coordinator
c) Complaints of Internet misuse and safety will be dealt with via the Trust's complaints procedure; this can be found on the Ebor website.
d) Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
e) Complaints related to child protection are dealt with in accordance with Trust child protection procedures.

The Trust adopts BECTA guidance on responding to safety incidents in school:



13. **Communication of Policy**

13.1 Pupils

a) Rules for Internet access will be posted in all areas where internet access is accessible.
b) Pupils will be informed that Internet use will be monitored.

13.2 Staff

a) All staff will be given the Ebor Academy Trust e-Safety Policy and its importance explained.
b) Staff will be made aware that Internet traffic is monitored
c) Professional conduct is essential.
d) All staff will sign to confirm that they have read and remain aware of the Staff Acceptable use Policy

13.3 Parents

a) Parents' attention will be drawn to Ebor's e-Safety Policy in newsletters, brochures and on the Ebor website.
b) The Trust will maintain a list of e-Safety resources for parents/carers
c) The Trust will ask all new parents to sign the parent/pupil agreement when they register their child with their school.

14. Associated Policies and Documents

a) IT Strategy
b) Acceptable Use Policy
c) Behaviour Policy (including Anti-Bullying Policy)
d) GDPR Policy
e) Ebor Academy Child Protection & Safeguarding Policies
f) Keeping Children safe in Education

Copies of Ebor Academy Trust Policies can be found on the website:
https://eboracademytrust.co.uk/policies/

15. Useful resources for teachers

BBC Stay Safe www.bbc.co.uk/cbbc/help/safesurfing/
Becta http://schools.becta.org.uk/index.php?section=is
Chat Danger www.chatdanger.com/
Child Exploitation and Online Protection Centre www.ceop.gov.uk/
Childnet www.childnet-int.org/
Cyber Café http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen www.digizen.org/
Kidsmart www.kidsmart.org.uk/
Think U Know www.thinkuknow.co.uk/
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

16. Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet www.childnet-int.org/
International "Know It All" CD http://publications.teachernet.gov.uk
Family Online Safe Institute www.fosi.org
Internet Watch Foundation www.iwf.org.uk
Parents Centre www.parentscentre.gov.uk
Internet Safety Zone www.internetsafetyzone.com