Online Safety Policy

Approval Date	June 2024
Policy Owner	Head of ICT Services and Infrastructure
Adopted by Trust Board	June 2024
Review Date	June 2025

CONTENTS

Section Page No.

Appendices

Introduction

This Online Safety policy applies to all settings in the 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 IT users.

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

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.

Further DfE guidance can be found here on the use of mobile phones in schools.

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.

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.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

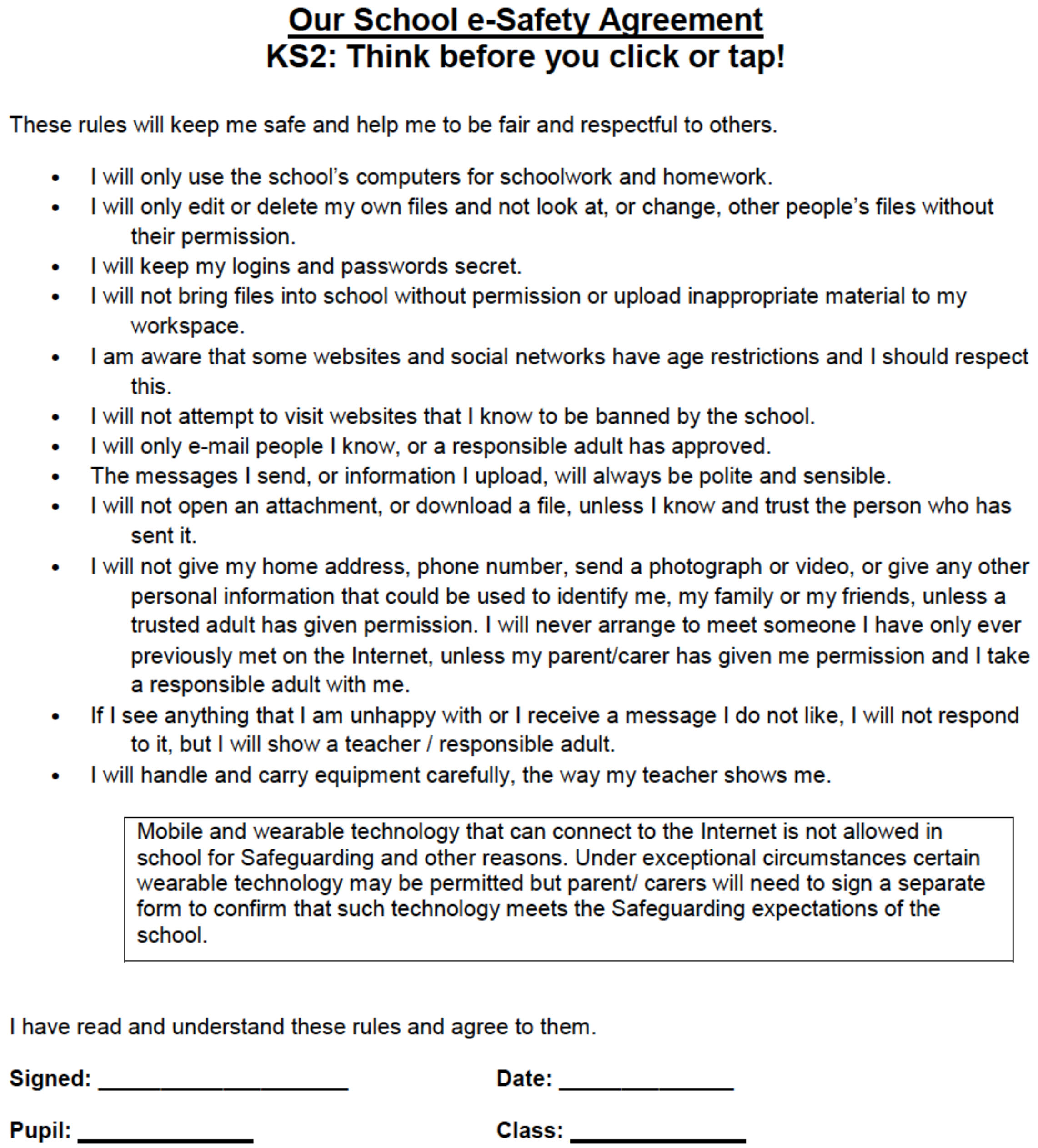
EYFS/KS1: Think before you

 S	I will only use computers and the Internet with an adult in the room
 A	I will only click on icons and links when I know they are safe
 F	I will only say kind things online
 E	If I see something I don’t like on a screen, I will always tell an adult

My Name:

My Signature:

Appendix 2: KS2 acceptable use agreement (pupils, parents/carers)



Our School e-Safety Agreement
KS2: Think before you click or tap!

These rules will keep me safe and help me to be fair and respectful to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit websites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything that I am unhappy with or I receive a message I do not like, I will not respond to it, but I will show a teacher / responsible adult.
- I will handle and carry equipment carefully, the way my teacher shows me.

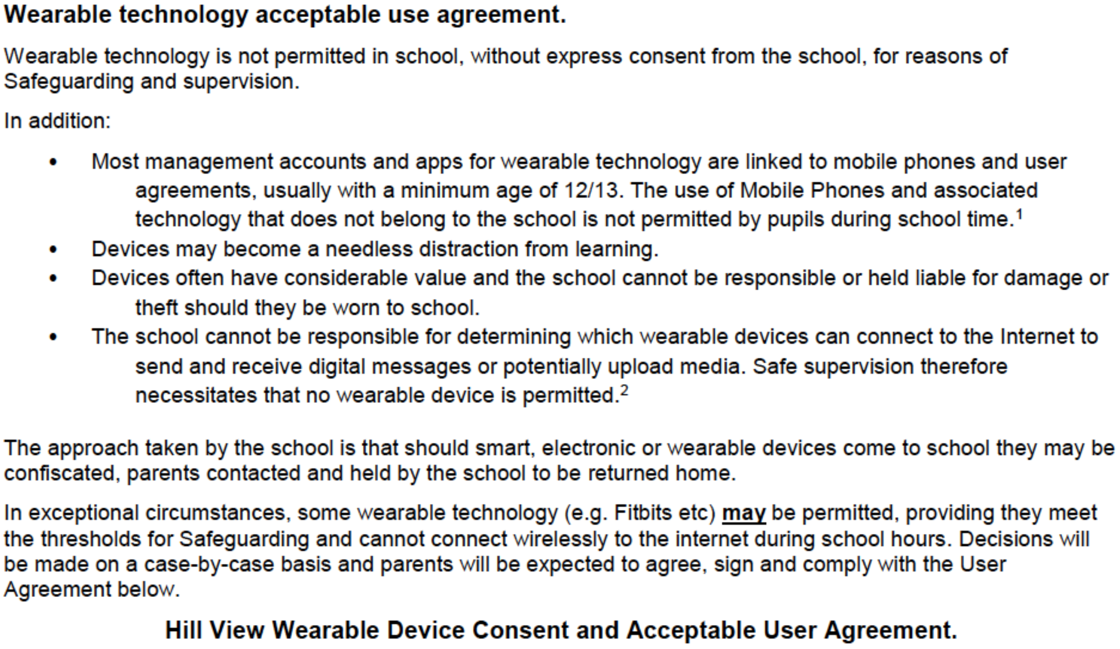
Mobile and wearable technology that can connect to the Internet is not allowed in school for Safeguarding and other reasons. Under exceptional circumstances certain wearable technology may be permitted but parent/ carers will need to sign a separate form to confirm that such technology meets the Safeguarding expectations of the school.

I have read and understand these rules and agree to them.

Signed: ____________________ **Date:** ______________

Pupil: ______________ **Class:** ______________

Appendix 3: Wearable Technology Acceptable Use Agreement



Wearable technology acceptable use agreement.

Wearable technology is not permitted in school, without express consent from the school, for reasons of Safeguarding and supervision.

In addition:

- Most management accounts and apps for wearable technology are linked to mobile phones and user agreements, usually with a minimum age of 12/13. The use of Mobile Phones and associated technology that does not belong to the school is not permitted by pupils during school time.[1]
- Devices may become a needless distraction from learning.
- Devices often have considerable value and the school cannot be responsible or held liable for damage or theft should they be worn to school.
- The school cannot be responsible for determining which wearable devices can connect to the Internet to send and receive digital messages or potentially upload media. Safe supervision therefore necessitates that no wearable device is permitted.[2]

The approach taken by the school is that should smart, electronic or wearable devices come to school they may be confiscated, parents contacted and held by the school to be returned home.

In exceptional circumstances, some wearable technology (e.g. Fitbits etc) **<u>may</u>** be permitted, providing they meet the thresholds for Safeguarding and cannot connect wirelessly to the internet during school hours. Decisions will be made on a case-by-case basis and parents will be expected to agree, sign and comply with the User Agreement below.

Hill View Wearable Device Consent and Acceptable User Agreement.

Child's name:_________________________ ___________Year____________ Class_____________

I can confirm that my child's wearable device:

- Complies with the thresholds for safeguarding and supervision at the Academy;
- Is not a true smart device (capable to downloading and running apps), merely a fitness tracker (such as a basic Fitbit type device).
- Is not able to wirelessly connect to the internet during school hours without the use of a connected phone.
- Is not capable of recording or playing media (including sound, photographs or video recordings) of any description, nor is it capable of downloading or uploading any text, sound or media to the Internet or any mobile network;
- Has no age recommendations related to it, or any software linked to it, that state that the user should be older than my child.

I understand that the school can take no responsibility for loss or damage of a wearable device and that misuse by my child will result in the device being confiscated and sent home.

This consent may be withdrawn by the school at any time.

I agree to the terms and to comply with this agreement:

Signed_______________________________________ Date:______________________

Print name_______________________________________

Approved: ____ Date:_______________

Role:______________________________

Appendix 4:Staff, Governors, Volunteers and Visitors Acceptable Use Agreement

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 which 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 pupils without checking with teachers first
- Share confidential information about the school, its pupils 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

Policy History

Date	Summary of change	Contact	Policy Implementation Date	Review Date
June 2024	Policy Implementation	Head of ICT Services and Infrastructure	June 2024	June 2025