Hilltop First School and Foundation Stage

E-Safety and responsible Internet Use Policy

SLT responsibility	LB
Reviewed by:	LB
Date:	March 2023
Approved by:	FGB

E-Safety and responsible Internet Use Policy

Contents

The school's Designated Online Safety Coordinator is Lynn Bima

The school's Designated Safeguarding Lead is Lynn Bima

The school's Deputy DSLs are Juliet Wright and Monica Romanay-Bhatt

Rational

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor RBWM can accept liability for any material accessed, or any consequences of Internet access.

Internet use will enhance and extend learning:

- The school Internet access is designed specifically for pupil use and will include filtering appropriate to the age of pupils.
- Clear boundaries are set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to use the Internet safely and responsibly using the following rules which the children are aware will help them to be fair to others and keep everyone safe:

- I will ask permission before entering any website, unless my teacher has already approved that site.
- I will not look at or delete other people's files.
- I will not bring flash pens, CDs or peripherals into the school without permission.
- I will not use internet chat.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell an adult immediately.
- I know that the school may check my computer files and may monitor the internet sites I visit.
- I understood that if I deliberately break these rules, I could be stopped from using the internet and computer.

These E-Safety rules will be posted in all rooms where computers are used. Safe use of digital technology, the internet and social media will be expletively taught during Computing and PSHE lessons.

Managing internet access

Information system security

- The School ICT system security and Virus protection are reviewed and updated regularly.
- If staff or pupils discover an unsuitable site, it must be reported to the Finance Manager who will advise the Internet Service Provider.

Published contents and the school website

- Staff or student personal contact information will not be published. The contact details given on-line are the school office.
- The Senior Leadership Team will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing pupils' images and work

- Pupils' images and names will only be used on a school website or other on-line space, with prior permission of parents.

Social networking and personal publishing

- No child under the age of 13 should have an active presence on a social networking site. Should the school become aware of such a presence, a member of the Senior Leadership Team will discuss this with the parents/carers.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils are not permitted to bring games machines into school.
- In some cases a parent may be given permission for a child to bring a mobile phone to school. In these rare cases, the phone will remained locked in the school office and will need to be collected by an adult at the end of the school day.
- Use of mobile phones forms part of our Staff Code of Conduct.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Policy decisions

Authorising Internet Access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. A signed copy of this form will be kept in individual staff personal files.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Handling e-Safety Complaints

- Complaints of Internet misuse will be dealt with by the Senior Leadership Team.
- Any complaint about staff misuse must be referred to the Headteacher.
- The school cannot be held responsible for any offensive use of email or social media sites outside of the school day. This must be managed through appropriate parental control.
- Pupils and parents will be informed of the complaints procedure.

- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- The school will work with Police when necessary.

Communicating e-safety

Staff and the e-Safety Policy

- All staff will be given the School e-Safety Policy.
- Staff are aware that network and Internet traffic can be monitored and traced to the individual user.
- Staff must maintain a professional standards in keeping with their role on any Social Networking sites.

Enlisting Parents' and Carers' Support

- Parents' and carers' attention will be drawn to the School E-Safety Polciyand Responsible Internet Use via the school website.

This policy is to be read in conjunction with the following school documents:

- Safeguarding and Child Protection Policy (Including Anti-bullying Statement
- GDPR Policy and Privacy Notice

Hilltop Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for their information and clarification.

- I understand that is it a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDA's, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to one of the Designated Safeguarding Leads.
- I understand that I will have no electronic communications with pupils including email, IM and social networking as this would be incompatible with my professional role.
- I understand that any electronic communication with other adults, including parents/carers via email, IM and social networking must be compatible with my professional role and ensure that messages cannot be misunderstood or misinterpreted.
- I will promote e-Safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT:

Signed: ………………………………………………… Date:……………………………………….

Staff Name: ……………………………………………. Staff Job Title: ………………………

Hilltop Staff Contract for Usage of Laptops

This contract should be read in conjunction with the Hilltop E-Safety and Responsible Internet Use Policy, and the Staff Code of Conduct for ICT.
Please read this contract carefully and sign at the bottom in order for you to be eligible to use a laptop at Hilltop.

- **Do not let any pupil use the laptop as it has been configured for staff use and has no restriction to the internet or network. Please note that all internet traffic is logged but not filtered.**
- You are responsible for all internet access on your computer when it is used at home. **Usage by non-staff is completely prohibited.**
- **You are not permitted** to install any software or internet access software on the laptop.
- **You must connect the laptop to the school network at least once a Month during term time** to keep it updated.
- **Ensure that you regularly update your documents to your S-drive and**
- **Do not eat or drink near your laptop** as you will be liable for any damage caused due to this and charged for the repair.
- **You are responsible for the laptop** – if the laptop gets stolen, it is covered by third party insurance but **the laptop is not covered for theft from a motor vehicle**. DO NOT leave your laptop in your car, if it gets stolen from your car, you will be liable for the replacement of this laptop. You need to let the Office Manager IT SUPPORT know immediately if the laptop is stolen to allow us to get a crime reference number from the police to enable us to get an insurance replacement.

Please note that failure to adhere to these conditions could result in your laptop being withdrawn.

Name: ……………………………………………………………………………………..

Signed: ……………………………………………………………………………………

Date: …………………………………………………………………………………

Laptop Make /Model: …………………………………………………………………….

Laptop S/N: ……………………………………………………………………………….

Laptop AD Number:……………………………………………………………………………