HILLSIDE INFANT SCHOOL

Online Safety Policy

Online safety links to child protection and safeguarding of both children and adults in the digital world. It is about learning to understand and use technology in a safe way. The internet is a wonderful resource for children but we have a responsibility to ensure that we support children and adults to develop safe online behaviour.

Online safety depends on effective practice at a number of levels:

- Responsible technology use, on and off-line, by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management appropriate filters.

Responsibilities

The Designated Safeguarding Lead, Mrs R Fennell, has overall responsibility for ensuring that all practices and procedures linked to any internet use are detailed and shared with staff.
It is the responsibility of each staff member to adhere to all guidelines in relation to safe and professional use of equipment, secure information sharing and minimising any known risk factors. Any breach of these guidelines, or suggestions for improvements, should be reported to the Safeguarding Lead.

Teaching and learning

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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. The school's Internet access is designed expressly for pupil use and includes age-appropriate filtering. Pupils will be taught what Internet use is acceptable and given clear objectives for Internet use. They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. If staff or pupils discover an unsuitable site, it must be reported immediately to the Safeguarding Lead and the school IT provider. The link for the site needs to be saved and the children prevented from seeing harmful content. Child Exploitation and Online Protection (CEOP) must be notified – there is a direct link on the school website. Any incident should be used as a teaching opportunity to explain to the children what has happened, what the danger was and what adults have done to protect the children.

Information system security

School ICT systems, capacity and security will be reviewed regularly and in accordance with national guidelines by the school's appointed provider of Internet Technology support. They will be responsible for virus protection, back-up and implementation of security strategies. Virus

protection will be automatically updated and verified regularly by the company responsible for IT support.

E-mail

Pupils may only use approved e-mail accounts on the school system. They must immediately tell a teacher if they receive offensive e-mail or do not recognise the sender. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone whom they do not already know in person. The only e-mail that children have access to in school is via Purple Mash which is a platform specifically designed for children.

Published content and the school web site

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Pupils' full names will not be used anywhere on the website in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Mobile phones

Pupils are not permitted to bring mobile phones into school. Mobile phones will not be used by adults during lessons. The sending of abusive or inappropriate text messages is forbidden. Mobile phones must never be used to take photographs of children. Contact with parents/carers should be made from the school landline. In the event of a mobile phone being used, caller ID must be blocked.

Protecting personal data

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

Authorising computer and e-mail access

All staff must read and sign the Acceptable Use Staff Agreement (Appendix 1) before using any school ICT resource. Staff will lose access rights to school e-mails and systems when their employment ends.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access. Any concerns about inappropriate material will be reported immediately to the Safeguarding Lead for investigation and to enable action to prevent repetition. Investigation will include establishing if there are any issues related to child protection issues or staff misconduct.

Introducing online safety to pupils and their families

Parents/carers will be encouraged to take an active role in educating their child/children about online safety. They will be supported to do this by making use of information on the school website and being signposted to relevant information in newsletters. There is a direct link on the school website to report harmful content.

Children will be taught about staying safe online using age-appropriate stories and activities and resources, book choices and ideas for parent/carer use will be published on the school website.

Approval date: 29.09.2021
Review Date: September 2026

APPENDIX 1 ACCEPTABLE USE STAFF AGREEMENT

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body.
- I will not reveal my password(s) to any unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system for communication with parents/carers. (office@hillsideinfant.org.uk or via Class Dojo)
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Headteacher (Designated Safeguarding Lead) and the School IT provider
- I will never use personal digital cameras or camera phones for taking and transferring images of pupils.
- I will ensure that any private social media posts that I create or actively contribute do not compromise my professional position.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will promote the school's online safety policy when working with children.
- I understand that all internet and network usage can be logged and this information could be made available to the headteacher on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent on-line policies.

Appendix 2: Hillside Infant School Staff Portable Device Agreement

- The employee named below ("the user") has been allocated a laptop or other portable device ("device") by Hillside Infant School ("the School").
- The device remains the property of the School and as such should be returned to the School either on demand or at the termination of any employment contract with the School. The School reserves the right to recall the device, or reallocate it to another user, at any time.
- The user will not sell, assign, transfer or otherwise dispose of the device and will return the device to the School in good working order.
- The user agrees not to remove, conceal or alter any device markings or tags or mark the device in any way that will reduce its security and/or value.
- The device is for curriculum and school related use only.
- The user accepts that they should take reasonable care of the device at all times.
- The user accepts responsibility for the physical security of the device and will always place the device in a carry case for transportation. As such, the machine is insured under the school's insurance policies.
- If the device is lost or damaged the user agrees to advise the School as soon as possible. If the device is stolen the user agrees to advise the School and the Police as soon as possible and gain a crime reference number in order for the School to make an insurance claim.
- Antivirus software is pre-installed to all laptops. The user agrees to keep this updated as advised by the School's IT provider in order for it to remain effective.
- The device will be returned to the School's IT provider for any maintenance work upon request.
- The user will ensure that all local data on the device is adequately backed up on the School's network.
- The user should familiarise themselves, and comply, with the terms of the Data Protection Act for storage of student information on the device. The School is registered under the 2018 Data Protection Act.
- The user agrees to adhere to all LA and School policies regarding appropriate use, data protection, computer misuse and health and safety issues.