HORRABRIDGE PRIMARY and NURSERY SCHOOL
Policies & Procedures

TITLE: Computing and E-Safety Policy

DOCUMENT MANAGEMENT

This document constitutes version 8 of the **Computing and E-Safety Policy** and was **reviewed** in November 2024 by the Governing Board.

The document is subject to **review in November 2026.**

Information and Communications Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

Websites

E-mail, Instant Messaging and chat rooms

Social Media, including Facebook and Twitter

Mobile/ Smart phones with text, video and/ or web functionality

Other mobile devices with web functionality

Gaming, especially online

Learning Platforms and Virtual Learning Environments

Blogs and Wikis

Podcasting

Video Broadcasting

Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet

technologies and that some have minimum age requirements, usually 13 years.

Some of the dangers they may face include:

- Access to illegal, harmful, or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including other children.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

At Horrabridge Primary and Nursery School (HPNS) we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

HPNS hold personal data on learners, staff, and other people to help them conduct our day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, Governors, visitors, and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, web cams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

External Monitoring

The school's Internet provider logs all Internet activity. Authorised Local Authority (LA) staff may monitor these logs.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the HPNS Disciplinary Procedure or, where appropriate, the LA Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's Office's (ICO) new powers to issue monetary penalties came into force on 6 April 2010, allowing the ICO to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act (DPA).

The data protection powers of the ICO are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher (HT). Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the HT.

Acceptable Use agreement

It is important that our children learn the importance of safety and the role they have to play in their self-protection and that of their friends and fellow pupils.

The following Acceptable Use statement displayed in all KS2 classrooms and the ICT suite has been developed and our children will be expected to follow it in KS1 and sign it in KS2. Parents will be sent a copy too.

I will only use ICT in school for school purposes.

I will only use my class e-mail address or my own school e-mail address when e-mailing or for logging onto cloud based school activities.

I will only open e-mail attachments from people I know, or who my teacher has approved.

I will not tell other people my passwords.

I will only open/delete my own files.

I will make sure that all computing contact with other children and adults is responsible, polite and sensible. This will include not using any chat facilities during learning times unless told to do so by a teacher.

I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.

I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community

I know that my use of ICT can be checked and that my parent / carer contacted if a member of school staff is concerned about my eSafety.

In order to have a consistent approach and understanding in the home and at school Parents and Carers of pupils in Key Stage 2 will be asked to action the statement below:

Dear Parent/ Carer

Computing including the Internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Headteacher

Parent/ carer signature

We have discussed this and …….....(child name) agrees to follow the eSafety rules and to support the safe use of ICT at School.

Parent/ Carer Signature …….……..

Class ……. Date ……

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

What applies to the children must equally apply to Staff, Governors and Volunteers and therefore those individuals must agree to, and sign, the following in conducting their professional or lay responsibilities when using any form of ICT.

Any concerns or clarification should be discussed with the HT.

I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes.

I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities

I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

I will not give out my own personal details, such as mobile phone number and personal e-mail address (as opposed to work email address), to pupils.

I will only use the approved, secure e-mail system(s) for any school business.

I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school or accessed remotely. Personal data can only be accessed remotely when authorised by the HT or GB. Removable media will not be used to transport data offsite.

I will not take a school laptop home unless approved by the headteacher for work purposes, such as remote learning or planning, and will lock my school laptop when it is not in use, for example during break or lunch times. If undertaking remote learning it is highly recommended to only use school provided equipment.

I will use a strong password whenever using technology for access to or storing personal data. (A strong password should be at least 6 characters. A combination of letters, numbers and symbols. And a mix of lower and upper letters.)

I will not install any hardware of software without permission of the Computing

leader.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or HT.

I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or HT.

I will respect copyright and intellectual property rights.

I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand this forms part of the terms and conditions set out in my contract of employment.

In addition, I agree to use care not to comment on any perceived negative aspects of the school on Social Media platforms and I understand that the preferred area for any positive comments would be the PTA's public Facebook page. This page is monitored by a designated person and inappropriate use of this page will not be tolerated and may result in action being taken against me.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…… Date ……

Full Name …….....(printed)

Job title . . . . . .

<u>Computer viruses</u>

Computer viruses are a fact of life, but can be hugely disruptive, and with that in mind the following guidance must be followed:

- All files downloaded from the Internet or received via e-mail, must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Remote Learning

Normal safeguarding advice applies if the teacher becomes aware of any potential safeguarding issue online.

Sometimes, staff might need to contact children individually, for example to give feedback on homework. Staff should only contact children during normal school hours, or at times agreed by the school leadership team.

Parents' or carers' email addresses or phone numbers will be used to communicate with children, unless this poses a safeguarding risk. School accounts will be used to communicate via email or online platforms, never teacher's personal accounts.

Staff must make sure any phone calls are made from a blocked number so teacher's personal contact details are not visible.

We will ensure parents, carers and children understand the benefits and risks of online lessons and get written consent for children to be involved.

Teachers creating video content should be aware of the environment they are recording in to ensure it is appropriate for children to see. Teachers should:

- Set their videos to "unlisted" so that only people who have the link (e.g. parents who you've emailed) will be able to see the video
- Set the audience as "Made for kids", so that adverts won't appear at the start of the video, and comments will be disabled.
- Videos should be shared through the Google Classroom Platform
- Parents should be made aware of online resources that will help create a safe environment for the child to work at home: https://www.gov.uk/government/publications/coronavirus-covid-19-

keeping-children-safe-online/coronavirus-covid-19-support-for-parents-and-carers-to-keep-children-safe-online

E-mail

The use of e-mail within school is an essential means of communication for both staff and pupils. Teachers are expected to check their school email daily on the days on which they are employed and not on other days, including weekends and holidays, unless in exceptional circumstances. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to experience the full computing curriculum, pupils must have experienced sending and receiving e-mails. They will also need to use their school email address in order to access cloud based learning.

E-mails created or received as part of a school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. E-mail accounts must be actively managed to ensure all e-mails of short-term value are deleted and they must be organised into folders to carry out frequent housekeeping on all folders and archives.

The forwarding of chain letters is not permitted in school.

All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus-checking attachments

The school has given all staff their own e-mail account to use for all school business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, e-mail histories can be traced. The school email account should be the account that is used for all school business

Under no circumstances should staff contact pupils, parents or conduct any school business using personal, non-work, e-mail addresses

All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account where appropriate.

Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.

Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

Staff must inform the HT if they receive an offensive e-mail

Pupils are introduced to e-mail as part of the Computing Scheme of Work

However, you access your school e-mail (whether directly, through web mail when away from the office or on non-school hardware) all the school e-mail policies apply

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

E-Safety Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the HT and GB have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is ***Martyn Harris.*** All members of the school community will be made aware of the post holder post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Devon LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Staff and Governors are updated by the Head/ eSafety co-ordinator and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, behaviour/pupil discipline (including the anti-bullying) policy. In addition, the PTFA and school both individually have a public Facebook page for the purposes of sharing information about school events with parents. The school has a designated person who is responsible for the monitoring of the content of each of these pages and any comments made. The

designated person for the PTFA page is the Chair of the PTFA and for the school page is Sarah Pascall.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote safety and the school provides opportunities within a range of curriculum areas to teach about safety***Safety Skills and Development***

New staff receive information on the school's acceptable use policy as part of their induction

All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community

All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Summary

This policy is by its very nature detailed and, in some circumstances, prescriptive.

It is a fact of life however that no matter how detailed, rigorous or prescriptive a Policy is, there can be no guarantee that it provides 100% protection.

IF IN DOUBT – CONTACT HT IMMEDIATELY.