E-Safety and Online Policy

HARRIS PRIMARY SCHOOL

Approved by:	Ian Groom (Head teacher)	**Date:** September 2023
Last reviewed on:	July 2023	
Next review due by:	September 2025	

Introduction

- E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology.

- The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.

- Use of email, internet messaging and blogs all enable improved communication and facilitate learning and the sharing of data and resources.

- Virtual Learning Environments (VLEs) provide children with a platform for personalised and independent learning.

- Current and emerging technologies used in the school and, more importantly in many cases, used outside of the school by children include:

  - The internet;
  - E-mail;
  - Instant messaging;
  - Webcam communication;
  - Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player);
  - Social networking sites;
  - Video broadcasting sites;
  - Chat Rooms;
  - Gaming Sites;
  - Music download sites;
  - Mobile phones with camera and video functionality;
  - Smart phones with e-mail, web functionality and cut down 'Office' applications.

Curriculum

- The New Primary Curriculum states that children should apply their ICT knowledge, skills and understanding confidently and competently in their learning and in everyday contexts and that they become independent and discerning users of technology, recognising opportunities and risks and using strategies to stay safe.
- Across all six areas of learning children learn how to:
  - Find and select information from digital and online sources, making judgments about accuracy and reliability;
  - Create, manipulate and process information using technology to capture and organise data, in order to investigate patterns and trends;
  - Explore options using models and simulations; and combine still and moving images, sounds and text to create multimedia products;
  - Collaborate, communicate and share information using connectivity to work with, and present to, people and audiences within and beyond school;
  - Refine and improve their work, making full use of the nature and pliability of digital information to explore options and improve outcomes.

Identified Risks

- Children might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails.
- Children might receive unwanted or inappropriate emails from unknown senders, or be exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites.
- Chat rooms provide cover for unscrupulous individuals to groom children.

Social and Educational benefits…

- Children are equipped with skills for the future.
- The Internet provides Instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The Internet helps to improve children's reading and research skills.
- Email, instant messaging and social networking helps to foster and develop good social and communication skills.

These far outweigh the risks involved and as a school we will ensure users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

Policies and Procedures

- The school's e-safety policy will operate in conjunction with other policies including: Behaviour, Anti-Bullying, Teaching and Learning and Data Protection/GDPR.
- Our e-Safety Policy has been written building on BECTA government guidance.
- The e-Safety Policy and its implementation will be reviewed annually and where necessary in cases of reported misconduct or risks.
- All school staff and pupils are to sign an Acceptable Use Policy (AUP) detailing the ways that staff, pupils and all network users should use our ICT facilities and reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. The AUP is displayed in all classrooms and on laptop trolleys.
- E-safety will form a key part of the ICT/PSHE Curriculum. Children will be made aware of the dangers and risks of using the Internet and mobile technologies throughout the school year.

Shared Network

- All staff must access the network using their own logins and passwords. These must not be disclosed or shared. The children will login using their year group's username.
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Software should not be installed without prior permission from the ICT Technician or subject leader.
- Removable media (e.g. pen drives/memory sticks and CD-ROMs) must be scanned for viruses before being used on a machine connected to the network. Pupils may send in files to class teachers by email.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.

- The school has a wireless network, which is encrypted to prevent outsiders from being able to access it.
- Staff must ask permission from the e-Safety Coordinator before installing software on any school machines, which should normally be installed by the Network Manager.

Filtering

- The school uses a firewall provided by Lancashire ICT/ CLEO.
- School can ask IT Support for sites to be added and deleted using Lightspeed.
- The school ensures that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to a teacher and the e–Safety Coordinator immediately.
- Senior staff regularly check to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal is reported to appropriate agencies such as CEOP.
- The school's access strategy is designed by educators to suit the age and curriculum requirements of the pupils.

Internet Access

- The internet is an essential element of 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 our curriculum and a necessary tool for staff and pupils.
- The school internet access will be designed expressly for pupil use and will use appropriate filtering system.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will not use the internet without having permission from a member of staff.
- All users must sign an Acceptable Use Agreement before accessing the internet in school.
- Parental or carer consent is given in order for children to be allowed to use the internet.
- The internet must only be used for professional or educational purposes.
- Children must be supervised at all times when using the internet.
- Procedures for safe internet use will be clearly displayed beside every computer with access to the internet.
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the Headteacher and a note of the offending website address (URL) taken so that it can be blocked.
- Internet use will be monitored regularly in accordance with the Data Protection Act.
- Pupils using the 'Internet Cafe' at break times will be supervised by staff at all times and strict guidance will be given on acceptable websites for these periods.
- Pupils will not use social networking sites in the school and will be educated about their safe usage in their own time.
- Pupils will be advised never to give out personal details of any kind, which may identify them, their friends or their location.
- Pupils are forbidden from downloading games or other programs from the internet.
- The ICT technician will carry out downloading programs from the internet.
- Public chat-rooms and instant messaging are not allowed and should be blocked using the school internet filter. Any concerns should be reported to the ICT coordinator immediately.
- Access to peer-to-peer networks is forbidden in the school.

    - Pupils will be educated in 'Information Literacy' and taught how to evaluate the internet content that they have located. Pupils will be taught the importance of crosschecking information before accepting its accuracy.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or the intellectual property of others.
- Pupils will be taught how to report unpleasant internet content.
- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.

E-mail

- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- All emails sent from a school email account will carry a standard disclaimer disassociating the school and the Local Authority with the views expressed therein.
- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails received should not be deleted, but kept for investigation purposes.
- When available, pupils may only use approved school e-mail accounts on the school network. Pupils are not permitted to use their own personal email accounts on school equipment.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known. All email attachments must first be scanned before they can be opened
- Staff should never use personal e-mail addresses to communicate with pupils. The ICT coordinator will provide an official school e-mail address.

Cameras, Video Equipment and Webcams

- Permission must be obtained from a child's parent or carer before photographs or video footage can be taken. In order to support this policy, we would ask parents/carers not to use any images of our pupils on social networking sites such as Facebook. This includes any professional photos that have been purchased through the school and any photos taken during school concerts or sports events. Your individual rights to use family pictures on social networking sites are not affected by this, although it is advisable to consider whether images posted on any websites could be copied and/or misused.
- Photographs or video footage will be downloaded immediately and saved into a designated folder.
- Any photographs or video footage stored must be deleted immediately once no longer needed.
- Staff will not use personal equipment to record images, unless they have permission to do so. Any adult using their own camera, video recorder or camera phone during a trip or visit must transfer and save images and video footage onto the school network immediately upon their return.
- Parents of any child will be allowed to record school performances (eg Nativity or Star Assembly) provided the recording is for viewing within that child's family and must not be shared on social media.

- When available, video conferencing and webcam use will be appropriately supervised.
- Pupils will be taught the dangers of using webcams outside of the school.
- Video conferencing equipment and webcams must be switched off (disconnected) when not in use and the camera turned to face the wall.

- Webcams must not be used for personal communication and should only be used with an adult present.
- Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

School Website

- The school website is provided for use of school staff, pupils and the wider community. Class teachers will strictly prohibit unacceptable use and have total editorial control of postings.
- All staff and pupils possess a username and password as a level of security. The correct levels of privilege are applied to the correct users.
- Activity on the school website will be monitored to ensure that the content posted by users is valid and does not infringe the intellectual property rights of others.

Published Content and the School Web site

- Staff or pupil's personal contact information will not be published. The contact details given online should be the school office.
- The class teacher will take editorial responsibility for their class page and ensure that content is accurate and appropriate.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school web site. Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Work can only be published with the permission of the pupil and parents.
- Pupil image file names will not refer to the pupil by name and should be securely stored on the school network.

Portable Devices

- Children are not permitted to have mobile phones in school without permission, and they should be switched off at all times during the school day and left in the school office.
- Staff are required to have their mobile phones on 'silent' during the school day and should only use them during their break times or with permission from the Head Teacher.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should be aware that technologies such as portable laptops and mobile phones may access the internet by bypassing filtering systems and present a new route to undesirable material and communications.
- Staff should not use their personal mobile phones to contact pupils or capture photographs of children, unless given permission to do so. Alternative equipment will be provided by the school.
- Pupils are taught how to protect themselves against becoming victims of theft and how to report such an event to the correct authority.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.
- Technologies such as mobile phones with wireless internet access can bypass the school filtering systems and present a new route to undesirable material and communications.
- Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access, which may not include filtering. These may not be used in the school.

Protecting Personal Data

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

Roles and Responsibilities

- The name of our e-Safety Coordinator is available from the school office.
- Support will be provided by the ICT technician. Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance; keeps the Headteacher, senior management and Governors updated as necessary; ensures that any e-safety concerns are reported in the first instance to the e-Safety Coordinator who will investigate the concern and take the appropriate action.
- Our Governors have an understanding of e-Safety issues and strategies at the school, and are aware of local and national guidance on e-safety and are updated at least annually on policy developments.
- Our staff have e-safety responsibilities: to be familiar with the policy and to adhere to its procedures and must be familiar with the school's policy in regard to:
  - Safe use of e-mail;
  - Safe use of internet;
  - Safe use of the school network, website, equipment and data;
  - Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
  - Publication of pupil information/photographs and use of the web site;
  - E-Bullying / Cyber bullying procedures;
  - Their role in providing e-safety education for pupils;
  - Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential;
  - Staff will always use a child friendly, safe search engine when accessing the Internet with pupils. (e.g. Google Safe Search – default settings).
  - GDP Regulations
- School staff will be reminded/updated about e-safety matters at least once a year.

Management of ICT

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale of linked 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.
- The school will continue to monitor the use of Internet, email and messaging services.

- The school should audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate.

- **Handling e-safety complaints**
- Complaints of Internet misuse will be dealt with by the e-Safety Coordinator.
- Any complaint about staff misuse must be referred to the Headteacher;
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding/child protection procedures (see Safeguarding/Child Protection Policy).
- Pupils and parents will be informed of the possible consequences for pupils misusing the internet.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

- **Enlisting parents' support**
- Parents' attention will be drawn to the school e-Safety Policy in newsletters and on the school web site.
- Parents will be given a copy of the Acceptable Use Policy that their child has signed. They will be encouraged and supported to monitor their children's use of technology at home.

- **Sanctions**
- If rules are broken the types of sanctions we intend to impose if procedures are not adhered…
- Letters may be sent home to parents or carers (if applicable).
- Users may be suspended from using the school's computers, Internet or email, etc. for a given period of time/indefinitely.
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.

- **Concluding Statement**
- As a school we are aware that the procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the establishment/service and that this policy will not remain static. It may be that staff/children might wish to use an emerging technology for which there are currently no procedures in place. It is therefore advisable to state that the use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy update.

The school has appropriate filters and monitoring systems in place regarding use of internet (3G and 4G) in school.

PREVENT

Under the Counter Terrorism and Security Act 2015, schools have a duty to "have due regard to the need to prevent people from being drawn into terrorism".

This school is mindful of our duty to PREVENT extremism/terrorism. To this end the British Values of tolerance, democracy, rule of law and individual liberty are promoted and taught throughout our procedures, policies and curriculum.

Schools should be safe places for children to discuss and understand these issues and this policy is not intended to limit discussions surrounding sensitive issues. However, **any visitors or speakers, whether invited by pupils or staff, must be suitable for primary age children and will be fully supervised by the class teacher during their time in school. School events will be checked by the Headteacher to ensure they will not pose a risk.**

The school has robust safeguarding procedures in place to identify children at risk and to intervene as appropriate. All areas of the curriculum will support diversity, welfare, equality and safety. Pupils will be encouraged to respect others with particular regard to the protected characteristics in the Equality Act 2010.

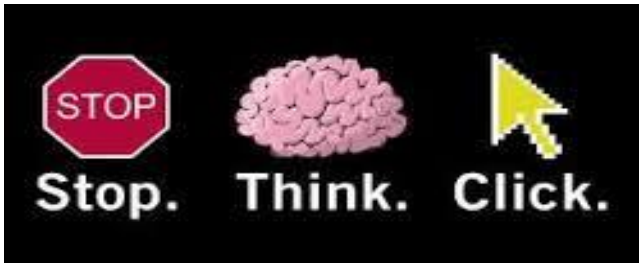
Any concerns regarding radicalism, extremism or terrorism must be reported to the Headteacher/DSL for Safeguarding immediately.

Appendix 2 – Internet Use

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Lancashire Grid for Learning
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Ask.com Safe Search Kids Google (monitored)
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. An e-mail address with protected password should be used.	Class email account Password held by class teacher
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified by name. File names should not refer to the pupil by name.	
Social Network sites.	No access allowed.	

Appendix 3 – Acceptable Use Policy

Poster to be displayed by all computers and explained to children:
KS2 children to read and sign AUP before using school computers.



These rules will keep everyone safe and help us to be fair to others.

- I will ask permission before entering any website, unless my teacher has already approved that site.
- On a network or permitted website, I will only use my own login and password, which I will keep secret.
- I will not look at, move, change or delete other people's files.
- I will not alter any computer settings, including passwords, screen savers, backgrounds, themes or locations of icons.
- I will not download software or apps.
- I will not bring digital files or storage devices to school without permission from school.
- I will only use the computers for schoolwork and homework.
- I will only e-mail people that my teacher has approved.
- The messages I send will be polite and sensible.
- 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 my teacher has given permission.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use internet chat or calls.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the internet or computers.

Websites to use at playtimes and lunchtimes:

Pupil Consent Form

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Harris Primary School **Acceptable Use Policy for ICT** Please complete, sign and return to school.	
Pupil:	Class:
Pupil's Agreement I have read and understood the school's Acceptable Use Policy for ICT. I will use the computer system and internet in a responsible way and obey these rules at all times.	
Signed: (by pupil or on behalf of pupil)	Date:
Parent/Carer's Consent for Internet Access I have read and understood the school's Acceptable Use Policy for ICT and give permission for my son/daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	
Signed:	Date:
Please print name:	
Parent/Carer's Consent for Web Publication of Work and Photographs I agree that, if selected, my son/daughter's work may be published on the school website. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not identify individuals and that names will not be used.	
Signed:	Date: