E-Safety and Acceptable Use Policy

2024-2025

Approved by:	Headteacher / IT Co-ordinator	**Date:** June 2024
Last reviewed on:	September 2024	
Next review due by:	September 2025	

Hale Preparatory School E-Safety and Acceptable Use Policy

Children must be safeguarded from potentially harmful and inappropriate online material. Hale Prep adopt a whole-school approach to online safety. It empowers the school to protect and educate pupils, students, and staff using technology and establishes mechanisms to identify, intervene, and escalate concerns where appropriate.

The breadth of issues classified within online safety is considerable but can becategorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate, or harmful content, for example, pornography, fake news, racism, misogyny, self-harm, suicide,anti-Semitism, radicalisation, and extremism.

- **contact**: being subjected to harmful online interaction with other users; forexample peer to peer pressure, commercial advertising, and adults posing as children or young adults to groom or exploit them for sexual, criminal, financial, or other purposes.

- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images(e.g. consensual and non-consensual sharing of nudes and semi-nudes and pornography, sharing other explicit images and online bullying.

- **commerce** - risks such as online gambling, inappropriate advertising,phishing, and financial scams. Support can be found here: (https://apwg.org/)

Teaching and learning

Internet Access

- The Internet is essential in 21st-century life for education, business, and social interaction. The school must provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the Hale Prep curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning.
- The school Internet access will be designed expressly for pupil use and will include filtering.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be 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 evaluate internet content.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

E-mail

- When available, pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In any e-mail communications, pupils must not reveal their details or those of others or arrange to meet anyone without specific permission.
- Incoming e-mails should be treated as suspicious, and attachments not be opened unless the author is known.
- The forwarding of chain letters is not permitted.

Published content and the school website

- Staff or pupil personal contact information will not be published. The headteacher will take overall editorial responsibility and ensure accurate and appropriate content.
- Pupils' full names will not be used in association with photographs anywhere on the school website.
- Pictures will only be shown on the website if parents/carers sign the consent form at the start of each school year.
- Parents will be informed of the school policy on image taking and publishing.

- Parents will have access to this policy through the school website, including a link to the Cyberbullying Policy.

Social networking and personal publishing

- In school, social networking sites will not be used.
- During IT e-safety lessons, pupils will be advised to:

    - Use nicknames and avatars when using social networking sites at home.
    - Never arrange to meet anyone on a networking site.
    - Not post pictures wearing school uniform.
    - Ask permission from those involved before posting pictures.
    - Only make 'friends' or chat with people they know and who are of similar age.
    - Never give out ANY information about themselves, e.g. phone number, address.

Responsibilities

- **All staff who use IT connected with the school has a responsibility to regard e-safety.**
    i) Teachers will not post images or names of children on social networking sites.
    ii) Teachers will not post any school-related information on their social media.
    iii) Teachers are not to accept friend requests from parents, current or former pupils.
    iv) Teachers' social media accounts should be set to private.
    v) Teachers will be responsible for deleting any photos they take of children on their mobile phones immediately after sending them to the IT coordinator and before they leave the premises.
    vi) It is the responsibility of the teachers to provide images/information for the school website. This should be posted on Instagram, emailed to the school office and then deleted.

    Disciplinary procedures will be taken if staff do not adhere to these responsibilities.

- The teaching staff has a responsibility to teach e-safety.
    The e-safety / IT teacher(s) will:
    i) oversee the review of this policy
    ii) oversee the implantation of this policy
    iii) advise the school management on e-safety issues

vii) advise staff on e-safety teaching and learning resources

viii) be a point of contact for any concerns about e-safety.

ix) pass on to the Head Teacher any complaints received concerning individuals orstaff misuse of ICT.

x) supervise the technician who manages the filtering systems/security systems.

xi) teach a block of 'e-safety' lessons in addition to ongoing instruction.

xii) ensure that all staff read and sign the "Acceptable Use of ICT - Staff" documentbefore using any school ICT resource. This will be renewed eachnew school year (normally in September).

Technical provision

- Hale Prep has "ESET End Point Security" installed on all its PCs to combat any possible virus. It also has Smoothwall S3 filter and monitoring system to filter and monitor inappropriate content to fulfil the school's safeguarding obligations. This is updated every evening. This will protect children from terrorist and extremist material when accessing the internetthrough school systems. On the iPads, DNS level filtering is observed. Weekly checks are carried out by technical support and are recorded in the computer room.

Protecting personal data

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998.
- Every staff member must take all reasonable steps to protect all data concerning pupils and others securely.
- Any data taken off the school premises should be kept to a minimum and deleted or destroyed appropriately or returned to school for destruction if no longer required.
- All printed copies of personal data must be shredded before disposal as waste material.
- Staff must take all reasonable care when using, storing, and transporting memory sticks. Where possible, all information must be stored on the shared drive and passwords deleted.
- Updated information is available in KCSIE Annex D on how to support keeping children safe online while learning at home.

Remote learning

Where children are being asked to learn online at home, the Department has provided

advice to support schools and colleges to do so safely: safeguarding in schools, colleges and other providers and safeguarding and remote education. The NSPCC and PSHE Association also provide helpful advice:

- NSPCC Learning –Undertaking remote teaching safely during school closures
- PSHE – PSHE Association coronavirus hub.

An annual review is carried out of this policy due to technology evolving rapidly and changing.

Reviewed September 2024

HALE PREP SCHOOL ACCEPTABLE USE POLICY –STAFF

Acceptable Use Policy Agreement

I understand that I must responsibly use school ICT systems to ensure no risk to my safety or the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will educate the young people in my care on the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the rules in this agreement also apply to using school ICT systems (e.g. laptops, email, etc) out of school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove, or otherwise alter other users' files without permission.
- I will use school email/team accounts or communication with parents during online learning.
- I will professionally communicate with others, not use aggressive or inappropriate language, and appreciate that others may have different opinions.
- I will ensure that when I take and publish images of others, I will do so with their permission.
- I will use chat and social networking sites in school for personal use.

Information shared should never compromise the school's duty to provide the highest possible standard of education or bring the school's reputation into

distribution. Staff with genuine concerns about any school matter should follow the school's current guidelines and policies, e.g. whistle-blowing to resolve issues and not networking sites. Staff should report all contacts through networking sites which may concern them to the headteacher. Examples may include a child below 13 on Facebook requesting to be a friend or inappropriate comments by a parent-directed to themselves.

- I will not post photographs of pupils on social media sites.
- I will only communicate with students/pupils and parents/carers

using official school systems. Any such communication will be

professional in tone and manner.

- I will not engage in any online activity that may compromise my professional responsibilities.
- When I use my handheld/external devices (laptops / mobile phones / tablets, etc.) in school, I will follow the rules set out in this agreement in the same way as if I was using school equipment. This includes downloading photographs on school computers. I will ensure that such devices are virus-free and protected by up-to-date anti-virus software.
- I will not use personal email addresses on the school ICT systems for pupils' data.
- I will not open any attachments to emails unless the source is known

and trusted due to the risk of the attachment containing viruses or

other harmful programs.

- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any illegal or inappropriate materials that may cause harm or distress to others. I will not try to use programs or software that might allow me to bypass the filtering/security systems to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not attempt to install programs on a machine or store programs on a computer, nor will I try to alter computer settings.

- I will not disable or cause any damage to school equipment or the equipment belonging to others.

- I will immediately report any equipment or software damage or faults to the Computing Teacher. However, this may have happened.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my work

- Where work is protected by copyright, I will not download or distribute

copies (including music and videos).

- I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school but also to my use of school ICT systems and equipment out of school and my use of personal equipment in school or situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

Updated September 2024