

Community Primary School Hampshire



E-Safety Policy

Adopted on:	May-26
Signed on behalf of the Governing Body	Mrs B Read Chair
Review Date	May-27

Cherrywood Community Primary School

E-Safety Policy

INTRODUCTION

ICT literacy has become an essential skill for everyday life. Technology is constantly evolving, and schools have to respond to these developments. This includes the rapid emergence of Artificial Intelligence (AI) technologies—from generative tools like Microsoft 365 Copilot and Google Gemini to embedded AI within learning platforms. The key to responding to these changes lies within the education system. It is the role of schools to model and teach ICT discretely and across the curriculum, with children leaving the school equipped to meet the demands of the ever-changing technological world.

This Policy sets out how the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology and AI tools;
- build both an infrastructure and culture of E-Safety and responsible AI literacy;

This Policy applies to all school community members (including Staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems and authorised AI platforms. The Policy highlights the need to educate pupils about the benefits and risks of using technology and provide safeguards and awareness for users to enable them to control their online experience.

AIMS

The aims of the school are:

- To provide children with the necessary knowledge and skills to make informed choices about using technology and AI beyond the classroom and after their time at school.
- To teach children to use relevant technology safely, including -
 - Feeling safe and confident when using new technologies and verified AI interfaces.
 - Knowing who to speak to when they feel unsafe or encounter unsettling AI-generated material/deepfakes.
 - Knowing how to report any abusive behaviour or algorithmic bias.
 - Knowing how to use the Internet and generative platforms correctly, without misuse.
 - Staying in control and keeping personal information private by never entering identifiable details into unauthorised AI prompts.
 - Knowing how to take the necessary measures to block and delete accounts, messages and people.

ROLES AND RESPONSIBILITIES

Governors

Governors are responsible for the approval of the E-Safety/AI Policies and for reviewing the effectiveness of the Policy. A member of the Governing Body has taken the role of ICT/AI and E-Safety Governor with responsibilities for the following: -

- Meetings with relevant Staff, including the Computing/AI Leader and Business/DPO Manager.
- Monitoring of E-Safety and AI misuse incident logs.
- Reporting relevant information to the Governing Body.

Headteacher and Senior Leadership Team

The Headteacher is responsible for E-Safety and AI governance, although day-to-day management affairs have been delegated to the Computing Leader and Business Manager.

The Headteacher and Senior Leadership Team ensure that all Staff receive correct and suitable Continuing Professional Development (CPD) including regarding emerging technologies and technical AI risks.

The Headteacher and Senior Leadership Team will ensure that there is a system in place to monitor the usage of the Internet and authorised AI tools and other technologies and that the person who carries out the internal E-Safety/AI monitoring receives support and is monitored. This provides a safety net and support to those colleagues who take on important monitoring roles.

The Headteacher and Senior Leadership Team will ensure that they receive regular updates and reports from the Computing Leader and Business Manager.

The Headteacher and Senior Leadership Team are to ensure they know the correct procedures that need to be followed concerning safeguarding or child protection.

E-Safety Team

The E-Safety team comprises the Computing Leader and the Business Manager, who are responsible for E-Safety issues and have a leading role in establishing and reviewing the school's E-Safety and AI policies/documents.

The E-Safety Team will ensure that all Staff are aware of the procedures that need to be followed in the event of an E-Safety incident or data leak via generative AI tools and will provide training and advice for all Staff.

The E-Safety Team will liaise with the Local Authority and Drift, the company the school uses to manage its network.

The E-Safety Team will receive reports of incidents including AI and create a log of incidents to inform future E-Safety developments.

The E-Safety Team will regularly meet with Governors to discuss current issues, review incident logs and report regularly to the Senior Leadership Team.

Technical Staff

The school uses Drift ICT and must comply with their email, internet and intranet policies. The filtering facility software is used to avoid access to inappropriate sites or material, including ensuring that AI chatbots cannot bypass school security filters. The school will partner with Hampshire County Council to ensure systems to protect pupils are reviewed and improved. Enforce technical guardrails that prevent the unauthorised export of downloading of internal school databases into public web-based AI tools.

Drift will provide technical support for the computer equipment that they supplied. The services provided by Drift include sourcing and supplying new hardware, providing weekly on-site support, installing and upgrading software, troubleshooting technical problems, maintaining the network, offering technical advice over the telephone and providing advice on strategic management of resources.

The school will comply with their "Policy on Acceptable Use of ICT" and any relevant Local Authority E-Safety Policies/guidance.

Teaching and Support Staff

E-Safety will be a focus in all areas of the curriculum, and Staff will reinforce E-Safety messages in using ICT across the curriculum. Teaching and Support Staff are responsible for.

- Staying up to date with current E-Safety matters, policies and practices.
- Reading, understanding, signing, and complying with the "Policy on Acceptable Use of ICT".
- Reporting any misuse or problems to the E-Safety Team / Headteacher for further investigation.
- Ensuring digital communications with pupils (email, Learning Platforms) are strictly professional and only carried out using agreed school systems.
- Ensure pupils are aware of and follow the E-Safety and Acceptable Use policies.
- Ensuring E-Safety issues relating to mobile phones, cameras, and hand-held devices are adequately monitored per the school's policies.
- Using only school-authorized AI tools [(e.g., Microsoft 365 Copilot, Arbot)] and strictly adhering to the permitted user base.
- Remaining "in the loop" during student interactions with technology, ensuring AI output complements rather than replaces human professional judgment.
- Reviewing and editing all AI-assisted materials used for lesson planning, grading rubrics, or report writing to guarantee factual accuracy and eliminate bias.
- **Never** uploading identifiable information about pupils (names, photos, addresses) or special category data into public, unauthorized tools.

In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material found in internet searches. Where pupils are allowed to freely search the Internet (e.g. using search engines) Staff should be vigilant in monitoring the content of the websites the pupils visit.

Designated Safeguarding Leaders

The Designated Safeguarding Leaders need to ensure that school staff are fully trained in E-Safety issues and are aware that serious child protection issues could occur due to: -

- Cyber-bullying.
- Sharing of personal data.
- Exposure to harmful AI-generated material (offensive, violent, or sexual content)
- Deception via AI deepfakes, synthetic media, or voice clone impersonations
- Algorithmic bias, radicalization, or automated grooming vectors
- Inappropriate online contact with adults/ strangers.
- Potential or actual incidents of grooming.

Pupils/

Pupils are responsible for-

- Knowing and acting accordingly to the school's E-Safety and Acceptable Use Policies.
- Knowing the importance of reporting abuse, misuse or access to inappropriate materials and knowing how to report them.
- Knowing the Policy on mobile phones, digital cameras and other hand-held devices and realising that these can be used for cyber-bullying.
- Understanding that the E-Safety policy also covers their actions out of school if related to their membership in the school.

Parents/ Carers

Parents and carers are responsible for ensuring that their children use the Internet and handheld devices such as mobile phones correctly and do not misuse these technologies. Full copies of the E-Safety and Acceptable Use policies are available from the school office and posted on the school's website. Parents/Carers are expected to comply with these policies.

Compliance with GDPR and School Privacy Policy

All Staff, pupils, parents/carers, volunteers, visitors and Governors are also required to comply with the School's Data Protection Policy and the Privacy Notices issued in accordance with that Policy in relation to the collection, retention, use of and sharing of the personal data of others (including but not limited to photographs, videos, identification data such as name, telephone numbers, addresses).

Any data misuse, policy breach, or notices (accidental or deliberate) must immediately be notified to the Data Protection Officer (the Business Manager).

EDUCATION

Pupils

The Internet is essential for education, business, and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for Staff and pupils. As such, the school has a duty to provide pupils with quality Internet access as part of their learning experience, which it will do in the following ways:-

- The school Internet access will be designed expressly for pupil use, including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.
- As part of the Computing curriculum, all year groups will be shown how to focus on the different elements of staying safe online.
- The school will ensure that the use of Internet-derived materials by Staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning, they will have been checked for appropriateness by the teacher setting the learning.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- Using **only** authorized AI tools under direct, supervised learning parameters.
- Never entering personal, sensitive, or family information into AI platforms.
- Adhering to strict academic integrity guidelines—refusing to use AI to plagiarize, cheat, or submit synthetic work as entirely their own design.

The school will ensure that all needs are met through ICT, considering gender, ethnicity, culture, religion, language, age, ability, disability and social circumstances. In this school, we must meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

Parents / Carers

Parents and carers will be informed about how the Internet and technology are used in school. They have a critical role to play in supporting their children with managing E-Safety risks at home, modelling appropriate behaviours, reinforcing key messages -and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear ICT acceptable use guidance and asking parents/carers to sign the school's Permission Forms.
- Raising awareness through information shared on the school's website
- Inviting parents to attend activities such as E-Safety and Computing events.

TRAINING OF STAFF AND GOVERNORS

There is a planned programme of E-Safety training for all Staff and governors to ensure they understand their responsibilities, as outlined in this Policy and Acceptable Use policies. This includes:

- An annual audit of the E-Safety training needs for all Staff.
- E-safety training for all new Staff as part of their induction programme.
- The E-Safety Team shares regular updates through, e.g. attendance at external training events and by reviewing guidance documents released from Hampshire County Council and other relevant organisations.
- This E-Safety Policy and its updates are being shared and discussed with Staff during the first INSET day of the academic year and throughout the year as appropriate.

- The E-Safety Team provides advice/guidance/training to individuals as required.

Governors will take part in E-safety training/awareness sessions in the following ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- Participation in school training/information sessions for Staff or parents, including attendance at assemblies/lessons.

TECHNICAL INFRASTRUCTURE

When working with the technical support provider, the school will ensure that the following guidelines are adhered to: -

- The School ICT systems are managed in ways that ensure that the school meets E-Safety technical requirements.
- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and workstations from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school will ensure regular reviews are made to ensure the filtering methods are appropriate, effective and reasonable.

The "Policy on Acceptable Use of ICT" provides clear explanations of technical and security aspects, including Access (Section 3), Unacceptable use (Section 8), Personal and private use (Section 9), Security and confidentiality (Section 10) and Monitoring (Section 11). The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that the Acceptable Use and E-Safety policies are implemented. It will also ensure that the relevant Staff will effectively carry out their E-Safety responsibilities.

DATA PROTECTION

The Data Protection Policy sets out how the school deals with personal information correctly and securely in accordance with the General Data Protection Regulations, which came into force in May 2018, and any subsequent amendments and other related legislation. In relation to E-Security, the school will adhere to the following: -

- At all times, take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password-protected computers and other devices.
- Ensure that users are correctly "logged off" at the end of any session in which they are accessing personal data.
- Store or transfer confidential data using encryption and secure password-protected devices only.
- Ensure data is deleted from the device once transferred or its use is complete.

USE OF DIGITAL AND VIDEO IMAGES

Photographs and videos taken within the school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's website and to provide information about the school on the website. The school will only take, store, use and share these photos and/or videos in accordance with the school's Data Protection Policy

and Privacy Notices and any restrictions in the Consent Forms completed by Parents/carers. In addition, the school will:

- When using digital images, instruct Staff to educate pupils about the risks associated with taking, using, sharing, publishing and distributing images on social networking sites.
- Allow Staff to take images to support educational aims, but make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Obtain written permission from parents or carers via the Consent Form before images or videos of pupils are electronically published.
- Keep the written consent where pupils' images are used for publicity until the image is no longer used.
- Ensure Staff will not keep images of children on personal devices, e.g. memory stick, or use them for any use other than in school.

COMMUNICATION

A wide range of rapidly developing communication technologies can potentially enhance learning. The "Policy on Acceptable Use of ICT" provides clear guidance on the acceptable use of these technologies, including emails, mobile phones, school telephones, Internet and social networking. The Acceptable Use Policy also provides information to Staff on ways to protect themselves from inappropriate use of ICT resources and equipment. The school will ensure that the Acceptable Use and E-Safety policies are effectively implemented.

ASSESSMENT OF RISK

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances, the school will examine and adjust this Policy. Part of this consideration will include a risk assessment:

- Looking at the educational benefits of the technology and
- Considering whether the technology has access to inappropriate material.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to internet content's global and connected nature, it is impossible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Hampshire County Council can accept liability for the material accessed or any consequences of internet use.

All users need to be reminded that using computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990, and breaches will be reported to the Police.

REPORTING AND RESPONSE TO INCIDENTS

The school will respond to illegal and inappropriate incidents as follows: -

- All members of the school community will be informed about the procedure for reporting E-Safety concerns (such as breaches of filtering, cyberbullying, and illegal content).
- Incidents of internet misuse by pupils and Staff will be referred to the Headteacher unless they consist of breaches of data protection legislation/the school's Data Protection Policy, in which case breaches must be reported immediately to the Data Protection Officer.
- Pupils and parents will be informed of the consequences for pupil misuse of the Internet (refer to Acceptable Use Policy).
- The E-Safety Team will record all reported incidents and actions taken in the School E-Safety incident log and in any other relevant areas, e.g. Bullying or Child Protection logs.
- The Designated Safeguarding Lead (DSL) will be informed of any E-Safety incidents involving child protection concerns, which will then be escalated in accordance with the school's Child Protection Policy.
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures.
- If investigations are needed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern that illegal activity has occurred (or the school is unsure how to proceed with any incidents of concern), then the school will contact the Hampshire County Council Children Services Team for support.

The Police will be informed where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images.
- promotion or conduct of illegal acts under the child protection, obscenity, computer misuse and fraud legislation.
- those covered by the Prevent agenda.
- adult material that potentially breaches the Obscene Publications Act in the UK.
- criminally racist material.

COMMUNICATION OF POLICY

Pupils

- Information on keeping safe online is shared throughout the school and discussed with children regularly.
- Pupils will be informed that Internet use will be monitored.

Staff

- All Staff will be given access to the school's E-Safety and Acceptable Use of ICT Policies and their importance explained.
- Staff should know that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

Parents

- Parents' attention will be drawn to the school's E-Safety Policy when their children first join the school, in school newsletters, e-safety briefings/updates, on the school website and through whole school events.

SANCTIONS AND DISCIPLINARY PROCEEDINGS

Sanctions and disciplinary procedures will be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- pornography, adult or mature content.
- promotion of any discrimination, racial or religious hatred.
- personal gambling or betting.
- personal use of auction sites.
- any site engaging in or encouraging illegal activity.
- threatening behaviour, including promotion of physical violence or mental harm.
- any other information which may be offensive to colleagues or breaches the integrity of the school's ethos or brings the school into disrepute.
- the use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Hampshire County Council and the school.
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties without the necessary licensing permissions.
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords);
- creating or propagating computer viruses or other harmful files.
- the breach of data protection legislation and/or the school's Data Protection Policy
- the breach of the Acceptable Use Policy.

OTHER SCHOOL POLICIES

This Policy should be read with other school policies, including the Acceptable Use of ICT, Child Protection, Anti Bullying, RSHE, Confidentiality, Whistle Blowing, Equality and Data Protection policies and Privacy Notices.