



ONLINE SAFETY ICT ACCEPTABLE USE POLICY



Document Status -

Policy Authors	Hollinswood Primary School & Nursery
Policy Created Date	May 2015
Policy Previous Review Date	June 2022
Current Policy Date	September 2026
Policy Review Frequency	Every Two Years
Date of Next Review	September 2028
Committee/Approver of Policy	Full Governors

Online Safety - Acceptable Use Statement of Practice

Introduction

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers, they may also arise through the use of games consoles, mobile phones, tablets and other handheld devices.

At Hollinswood Primary School and Nursery we ensure that we have in place appropriate policies and statements of practice to promote the safety of our learners; both when they are in the school and when they are elsewhere. We wish to encourage and support the positive use of ICT to develop curriculum and learning opportunities in school. However, as a professional organisation with responsibility for children's safeguarding, it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

In school we regularly deliver assemblies on keeping safe online, as well through lessons in class. The school has a duty to keep pupils safe from radicalisation and extremism. The school also has a duty to protect pupils from harmful online content, online abuse, cyberbullying, misinformation and disinformation, inappropriate use of artificial intelligence (AI), online exploitation and exposure to harmful material. Online safety is recognised as a safeguarding responsibility and forms part of the school's wider safeguarding framework. The school maintains appropriate filtering and monitoring systems in line with Department for Education expectations. Filtering and monitoring systems are reviewed regularly to ensure they remain effective, proportionate and age appropriate.

School ensures filters and monitoring systems are set so if devices are sent home, school internet search filters are maintained at home. Therefore any device taken home by a member of staff or pupil will not have access to inappropriate searches which may include sexual content, social network access, radicalisation, terrorism and extremism.

All staff have annual online safety training and any staff who have concerns are aware of their duty to refer to the Designated Safeguarding Lead who is also the Online Safety lead.

Mobile phones

Hollinswood Primary School & Nursery is a mobile phone-free environment. Pupils must not have access to mobile phones, smart watches with communication functions, or similar smart devices during the school day, including lessons, transitions, breaktimes and lunchtimes. Where an agreed exception exists for safeguarding, medical or travel purposes, devices must be switched off and handed into the school office for secure storage until the end of the school day.

Aims

This policy is designed to ensure that members of staff are fully aware of their professional responsibilities when using any form of ICT.

Professional Conduct Online

Staff, volunteers, governors, visitors and contractors are reminded that behaviour online should reflect the same professional standards expected within school. Offensive, discriminatory, threatening, defamatory or otherwise inappropriate online conduct may be treated as a disciplinary matter and could be referred to external agencies where appropriate.

Online Safety Rules for Foundation Stage

- I will take care of school computing equipment. If I spot any damage, I will tell my teacher.
- I will only use the program or website that my class is working on.

Online Safety Rules for KS1

- I will take care of school computing equipment. If I spot any damage, I will tell my teacher.
- I will only use the program or website that my class is working on.
- I will use my own login and password and will not share my password with others.
- I will treat other children's work with respect.
- I will tell an adult if I see anything online that I am uncomfortable with.
- I will remember to follow the online safety rules at home.

Online Safety Rules for KS2

- I will take care of school computing equipment. If I spot any damage, I will tell my teacher.
- I will use my own login and password and will not share my password with my others.
- I will not go on inappropriate sites. If I do this accidentally, I will tell my teacher.
- I will tell an adult if I see anything that I am uncomfortable with online.
- I will make sure I am respectful when writing online and will always use positive comments.
- I will make sure I do not copy anyone else's work or information from the internet and pretend it's my own.
- I will remember to follow the online safety rules at home.
- I will only use the names and pictures of my friends if they say it's OK.
- Out of school, I know I must not arrange to meet anyone that I don't know.
- If I bring a mobile phone to school, I will make sure that it is turned off and stored in the school office.
- I will only use artificial intelligence (AI) tools when a teacher permits it.
- I will not use AI to create harmful, offensive or inappropriate content.
- I understand that information produced by AI may not always be accurate and should be checked with a trusted adult or teacher.

Acceptable Use Policy for school staff and volunteers

Any messages, photos, videos or other media I post online will be out of my control. Any inappropriate searches on the internet will be reported to school. I agree that I will not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - Pornography (including child pornography)
 - Promoting discrimination of any kind
 - Promoting racial or religious hatred
 - Promoting extremism and radicalisation
 - Promoting illegal acts
 - Breach any Local Authority/School policies, e.g. gambling
 - Do anything which exposes children in my care to danger
 - Any other information which may be offensive to colleagues
- Forward chain letters, breach copyright law, do anything which exposes children to danger including, take images of pupils out of the premises on removable media or taking sensitive pupil information off the premises on removable media that is not encrypted

When using ICT equipment, I will not:

- Give anyone access to my login name or password
- Attempt to introduce any unlicensed applications
- Corrupt, interfere with or destroy any other user's information
- Release any personal details of any colleague or pupil over the Internet
- Use the school internet access for business, profit, advertising or political purposes
- Leave my account open at the end of a session – remember to 'lock' the screen

When using Artificial Intelligence (AI) tools, I will:

- Only use AI systems that have been approved by the school.
- Never enter confidential, personal, safeguarding or sensitive school information into public AI systems.
- Always review and verify AI-generated content before using it in educational or professional work.
- Ensure that any use of AI complies with safeguarding, data protection and copyright requirements.
- Be transparent where AI has significantly contributed to planning or content creation.

When using email I will:

- Only communicate with pupils, parents/carers and other professionals via a school provided email address or telephone number or via the message function on ClassDojo

- Observe 'network etiquette' on all occasions. Email or messaging should not be considered a private medium of communication and great care should always be taken over content, because of the possibility of public scrutiny
- Make sure that nothing in messages could be interpreted as libellous
- Not send any message which is likely to cause annoyance, inconvenience or needless anxiety

When working on professional documents that contain school-related information I will:

- Ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018.
- Not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones or memory sticks), unless they are secured and encrypted
- Protect the devices in my care from unapproved access or theft
- Not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- When using Artificial Intelligence (AI) tools, I will:
- Only use AI systems that have been approved by the school.
- Never enter confidential, personal, safeguarding or sensitive school information into public AI systems.
- Always review and verify AI-generated content before using it in educational or professional work.
- Ensure that any use of AI complies with safeguarding, data protection and copyright requirements.
- Be transparent where AI has significantly contributed to planning or content creation.
-

When using outside systems, I will:

- Make sure that any information I share on social networking sites takes into account my role as a member of staff
- Not allow pupils to be "friends" with me on social networking sites
- Keep data about students safe and be responsible for ensuring that the data protection act is not breached
- Consider that all online activity may be linked to my professional reputation and the reputation of the school.
- Never share confidential school information, safeguarding information or information relating to pupils online.
- Ensure privacy settings are regularly reviewed on personal social media accounts.
- Not communicate with current pupils through personal social media, messaging applications or gaming platforms.

This policy applies to both fixed and mobile internet; technologies that are in school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by staff that are brought onto school premises (such as laptops, mobile phones, memory sticks etc).

The school's ICT systems and network cannot be regarded as private, and user accounts will be subject to random monitoring. They should be used primarily for school purposes, but occasional personal use is permitted. All ICT activities must conform to the norms of moral decency and not contravene ICT or other relevant legislation.

ICT Acceptable Use Policy Agreement for Staff

- I have read, understood and accept the ICT Acceptable Use Policy. I agree that all members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner.
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I also understand that if I am found to have contravened any of these requirements that I may face disciplinary action.
- I accept that my use of the school IT facilities are monitored and the outcomes of the monitoring may be used.

Name:

Signed:

Date:

Acceptable Use Policy for **VISITORS AND CONTRACTORS**

We ask all children, young people and adults involved in the life of Hollinswood Primary School & Nursery to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

All staff (including support staff), governors and volunteers have legal / professional obligations, and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

All staff, governors and volunteers should read Hollinswood Primary School and Nursery full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to Mrs Osborne (Headteacher/DSL) or one of our Deputy DSLs

What am I agreeing to?

1. I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's systems security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
2. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
3. I will keep personal mobile phones and smart devices securely stored and out of use whilst working in areas occupied by pupils unless specific authorisation has been granted by the Headteacher or delegated member of staff. Under no circumstances will I use it (or other

capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member of staff.

4. If I am given access to school-owned devices, networks, cloud platforms or other technology:
 - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use.
5. I will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of my role.
6. I will not attempt to make contact with any pupils/students or to gain any contact details under any circumstances.
7. I will protect my username/password and notify the school of any concerns.
8. I will abide by the terms of the school Data Protection Policy and GDPR protections.
9. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
10. I will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.
11. I will not do or say anything to undermine the positive online-safety messages that the school disseminates to pupils and will not give any advice on online-safety issues unless this is the purpose of my visit and this is pre-agreed by the school.
12. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).
13. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

To be completed by the visitor/contractor:

I have read, understood and agreed to this policy.

Signature/s: _____

Name: _____

Organisation: _____

Visiting/accompanied by: _____

Date/time: _____

To be completed by the school (only when exceptions apply):

Exceptions to the above policy: _____

Name/role/date/time: _____

