

Community Primary School Hampshire



ICT Acceptable Use Policy

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

Cherrywood Community Primary School

Acceptable Use of ICT Policy

1.0 Introduction

This document outlines the school's policy on using telephones, email systems, internet, authorized Artificial Intelligence (AI) platforms and other technologies. The policy has been devised to enable pupils and staff to benefit from ICT (Information and Communication Technology), protect the school from potential legal liabilities and inform staff, pupils, parents and others about how they may use ICT appropriately in school.

ICT in the 21st Century is seen as an essential resource to support learning and teaching, playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies to arm our pupils with the skills to access lifelong learning and employment.

At Cherrywood, we understand the responsibility to educate our pupils on eSafety and AI literacy issues, teaching them the appropriate behaviours and critical thinking skills to remain safe, ethically aware and legal when using the internet and related technologies in and beyond the classroom context.

2.0 Application

- 2.1 This policy applies to all employees, governors and volunteers (collectively referred to as school staff within the body of the policy, as appropriate to their roles and responsibilities), as well as to parents/carers and pupils. The policy applies to all ICT, resources and equipment within the school, resources that have been made available to staff for working at home, and the use of personal IT equipment in school or on school-related matters. ICT resources and equipment include computer resources, use of school internet access, email systems and messaging systems, software (including use of software such as SAP, SIMS, Microsoft 365 Copilot, and Arbot), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic, algorithmic or communication equipment used by pupils when in school and by school staff in the course of their work.
- 2.2 This policy also provides advice concerning the potential risks and consequences in relation to inappropriate use of personal ICT facilities/equipment (including mobile telephones) by staff and others, where this use is inconsistent with the expectations of staff working with children and young people, and/or in breach of other school policies.

3.0 Access for Staff

- 3.1 School staff will be provided with a log on where they are entitled to use the school ICT facilities and advised what hardware, software and AI tools they are permitted to access, including access to the internet and email. Unless indicated, staff can use any available facilities subject to the facilities not being in use by pupils or other colleagues. Access is

provided to enable staff to perform their role and enable the wider school staff to benefit from such facilities.

- 3.2 Where staff have been provided with a school email address to enable them to perform their role effectively, it will only be used to communicate with parents and pupils if express permission has been provided.
- 3.3 Access to particular software packages and systems (e.g. HCC intranet; SAP (HR, finance and procurement system), SIMS, ASP, FFT, school texting services, Arbor) will be restricted to nominated staff. Without permission and access, staff must not access these systems. Similarly, direct access to school-supported AI platforms is restricted to authorized staff who have completed required training. Staff must not independently register school email addresses or upload school data to any "Unauthorized AI Tools" (any AI tool not formally assessed with a completed Data Protection Impact Assessment (DPIA)). Access to other software packages and information held electronically by the school, including but not limited to child protection/safeguarding records, will be given only in accordance with the school's Data Protection Policy and Privacy Notices.
- 3.4 Some staff may be provided with laptops and other equipment to perform their role. Where provided, staff must ensure that their school laptop/other equipment is not accessible by others when in use at home and that it is not misused by themselves or others. Staff must also ensure they bring their laptops/equipment to update software, licences and virus protection. When working offsite, data of a personal nature, as described in the school's Data Protection Policy, may only be used and stored through a school laptop working remotely or an encrypted memory stick (purchased by the school and allocated to staff). Staff are strictly prohibited from exporting, downloading, or copy-pasting personal or academic student data into public generative AI tools to generate text, analysis, or reports.
- All staff members should change their password from the generic one provided at the start of their employment and ensure that this is secure and changed regularly. Computers should also be locked when they are not actively in use.
- 3.5 Where the school provides digital equipment for educational and school business use, and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that parents have provided consent and that the school's policy in relation to Data Protection is followed.
- 3.6 Staff may use their personal mobile telephones in urgent or emergency situations during offsite visits. Where used in these situations and a cost is incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst offsite, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff with access to colleagues' personal contact details must ensure they are kept confidential.
- 3.7 No mobile telephones or similar devices, even those with hands-free facilities, must be used whilst driving on school business.

- 3.8 Staff should seek approval to access the school's telephone system for personal use. Where such use is made of this facility, it must be done during break periods, must not be excessive, and the school should require either the cost of the call or a donation to be made towards the cost of the call.
- 3.9 The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.
- 3.10 AI Notetaking and Meeting Recording: AI-powered notetaking tools or automated transcription assistants (e.g., within Microsoft Teams or Google Meet) may only be used if a formal DPIA has been approved, all participants are notified in advance, and explicit consent is granted. If external parties (parents, external professionals) object, the tool must be disabled

4.0 Communication with parents, pupils, and governors

- 4.1 The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring approval before use or agreeing on consent. The school must indicate to staff if any other individuals are permitted to make contact using the systems below:
- 4.1.1 School Telephones – all teachers, administrative staff and staff permitted through their roles in pupil welfare or a home/school link staff. Normally, teaching assistants and lunchtime supervisory staff would need to seek approval from a senior leadership team member where they feel they need to make a telephone call to a parent.
- 4.1.2 Text System (Teachers to Parents) – the Admin and Senior Leadership Team. Where other staff need to send a text, this is normally approved by a member of the Senior Leadership Team / Administrative Team.
- 4.1.3 Letters – all teachers may send letters home, but they must have these approved by the Headteacher/Deputy Headteacher before sending them. Where office staff send letters home, these will require approval similarly. Letters will be sent via email only wherever possible for correspondence that does not need parents to sign and return a slip.
- 4.1.4 Email – school email accounts should not be used for communication with parents unless approved by a senior leadership team member. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with staff members, communication may occur via email.
- 4.2 School staff should not use the methods outlined above to communicate directly with pupils if a staff member needs to contact a pupil directly via these methods. In that case, this must be approved by the Headteacher.

- 4.3 Where pupils or parents submit work electronically to school staff, this must be undertaken using school systems and not via personal email.

All communications must comply with the data protection legislation (including the Data (Use and Access) Act 2025 and the school's Data Protection Policy and Privacy Notices. Notification of any breach of this policy or the underlying regulations must be immediately to the Data Protection Officer, who is the school's Business Manager.

- 4.4 AI-assisted communications: Staff may use authorized Altools (e.g., Microsoft 365 Copilot) as an administrative aid to draft generic letters, emails, or newsletter items. However, staff must read, review, and edit all AI-generated text to ensure factual accuracy, appropriate tone, and alignment with school values before sending. Staff remain personally and professionally accountable for any text distributed under their name or the school's banner.

5.0 Social Networking

- 5.1 School staff must exercise extreme care in their personal use of social networking sites, considering their professional role in working with children. This includes ensuring they do not publish synthetic media, deepfakes, or AI-manipulated imagery that targets or references Cherrywood staff, pupils, or families, or brings the school into disrepute. Staff should use the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

- 5.2 No school staff should have pupils or ex-pupils under 18 as friends on their social networking sites. School staff are strongly advised not to have online friendships with young people (i.e., those at other schools) under 18 unless they are family members.

- 5.3 Where school staff accept friendships via social networking with ex-pupils aged over 18, they are advised to notify the Headteacher.

- 5.4 School staff are strongly advised not to accept friendships via their social networking with parents, ex-parents, and governors. Where staff accept such friendships, they must not discuss the school, whether expressing personal views or opinions, simply recounting events, or stating facts.

- 5.5 School staff can accept friendships with colleagues via their social networking site. Still, they should take care in communications exchanged. They must not engage in discussions regarding the school, whether expressing personal views or opinions, simply recounting events or stating facts. Senior staff and those with line management responsibility are advised to consider the appropriateness of accepting colleagues, particularly those they manage, as friends on social networking sites. Where accepted, staff should take care to exercise discretion in relation to the communications exchanged.

- 5.6 When school staff become aware that there is information about them held on social networking sites that causes them personal concern, they should alert the Headteacher.

Staff should also notify the Headteacher if they become aware of any material or exchanges on any form of social media which are in breach of this policy, the school's Privacy Notices and the school's policy on publication of photographs/videos etc, and/or which might give rise to safeguarding/child protection concerns relating to any pupil in the school, or which might damage the reputation of the school.

6. Pupil Use of ICT

- 6.01 The school makes access to it available to all pupils via the school's iPads, Chromebooks and classroom computers.
- 6.02 Access is for educational purposes only.
- 6.03 Independent Pupil AI Use Prohibited: In accordance with platform age limits and Key Stage requirements, pupils in Key Stage 1 and Key Stage 2 are strictly prohibited from independently accessing or creating accounts on public, commercial generative AI platforms (e.g., ChatGPT, Gemini). Pupils will experience AI concepts exclusively through highly structured, teacher-guided demonstrations or within safe, school-approved educational applications
- 6.04 Access is for educational purposes only and may include conducting research, playing educational games, and producing electronic presentations, films and audio of their work. At the staff's discretion, pupils may be allowed access to the internet/online games, etc, in break times or otherwise outside of lessons. This access is subject to this policy and controlled and supervised like during lessons. Recording of information by pupils electronically is subject to the Data Protection Policy and Privacy Notices provisions.
- 6.05 As teachers plan a particular lesson, they will evaluate suitable websites. Details of suitable sites will be added to schemes of work for future use. When using the internet, younger children may be restricted to using specific websites chosen by the teacher. As children become more experienced and proficient, they may be permitted to wider access, using search engines. An adult must supervise every pupil to use the internet. Informally when opportunities arise and formally as part of the Online Safety curriculum, educating pupils on the dangers of technologies that may be encountered outside school. Our ICT curriculum will include guidance and reminders about safe internet and core AI literacy, , helping pupils evaluate the reliability of information, understand algorithmic bias, spot AI "hallucinations," and identify deepfakes. They will be delivered in a way appropriate to the pupil's age and the level at which they will likely be accessing the internet.
- 6.06 The school's internet service provider, Harrap, provides a filtering service that does not allow access to sites considered unsuitable. Whenever staff are made aware of any site unsuitable for school use, the headteacher or school's network manager should be informed immediately. They will pass on the information to Harrap to make appropriate changes.
- 6.07 Any pupil found trying to access inappropriate information or deliberately using unauthorized AI tools to cheat, falsify assessments, bypass internet filters, or generate

harmful/bullying content will be sanctioned in accordance with the school's behaviour policy and may lose all privileges to use IT for such period as the Headteacher determines, depending on the nature of the incident(s).

- 6.08 Children are expected to follow the rules in the school's Mobile Phone Policy, with parents supporting these expectations. In particular, pupils understand what child-on-child abuse is. They will not use their phones to take and share photos or videos of others without their permission, especially on social media, nor take part in any digital messaging that breaches the school's Mobile, Anti-bullying and/or Behaviour policies. For programmes enabling children to communicate with others, they will behave safely and respectfully, reporting any concerns.
- 6.09 Pupils must not send friendship requests to or be friends with any staff member (unless they are over 18 and/or that staff member is also a relative or family friend) on any form of social media. If a pupil is a friend on social media of any staff member, in that case, they must not discuss matters relating to the school, school staff, other pupils or families of the school on social media.
- 6.10 Pupils must not share any password or other log-in information they use to access school-based/provided IT systems or programmes with other pupils or people outside the school (other than parents/carers).

7.0 Parent Use of ICT

7.01 Parents are expected to:

- Follow the behaviours shared in the school's Mobile Phone Policy, Data Protection Policy and Privacy Notices;
- Support the school in its delivery of safe and appropriate use of ICT, including social media and reinforcing safe boundaries around generative AI use at home; parents are expected to model acceptable behaviour themselves;
- Having taken appropriate action following any incidents outside of school, parents are encouraged to inform the school to support children as required.

8.0 Unacceptable Use

8.1 School systems and resources must not be used under any circumstances for the following purposes:

- 8.1.1 To communicate confidential information to the school or to communicate/share confidential information which the staff member does not have authority to share, including personal data as defined in the General Data Protection Regulations and the school's Data Protection Policy.
- 8.1.2 To present any personal views and opinions as the views of the school or to make any comments that are libellous, defamatory, false or misrepresent others

- 8.1.3 To access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material
- 8.1.4 To communicate or post anything via ICT resources and systems, including social media, that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally
- 8.1.5 To communicate or post anything via ICT resources and systems, including social media, that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils
- 8.1.6 To upload, download, post, email or otherwise transmit, share or store material that contains software viruses or any other computer code, files or programs designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or to input proprietary school data, database structures, or source files into unauthorized public platforms.
- 8.1.7 To collect or store personal information about others without directly referencing the General Data Protection Regulations and the school's Data Protection Policy.
- 8.1.8 To use the school's facilities to undertake any trading, gambling, or other action for personal financial gain or political purposes, unless as part of an authorised curriculum project.
- 8.1.9 To visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the school.
- 8.1.10 To undertake any activity (whether communicating, accessing, viewing, sharing, uploading or downloading) which has negative implications for safeguarding children and young people.
- 8.1.11 To present AI-generated content or text as entirely one's own authentic professional or academic work in formal contexts (Plagiarism/Academic Dishonesty).
- 8.1.12 To generate, process, or disseminate synthetic media (deepfakes, voice clones, or manipulated biometric content) intended to deceive, defame, harass, or impersonate any member of the school community.
- 8.1.13 To upload a student's creative work, writing, or intellectual property into external networks for the purpose of training commercial AI models without verified parental consent.
- 8.2 Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. Suppose employees need clarification about the use of ICT resources, including email and the intranet. In that case, advice should be sought from a member of the Senior Leadership Team or ICT lead if applicable.

- 8.3 Where an individual accidentally accesses a website or material that they consider to be pornographic or offensive or is otherwise in breach of this policy, this should be reported immediately to the Headteacher or other member of the senior leadership team, or if a breach of data protection legislation and the school's Privacy Policy, to the Data Protection Officer (the school's Business Manager). The school uses the Harrap filtering facility software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team applies where school staff use school equipment or facilities at home and accidentally access inappropriate sites or material.
- 8.4 Where an individual has been communicated with in a manner outlined above (e.g., has received an inappropriate email or attachment), they are advised to report this immediately to the Headteacher or another senior leadership team member so that this can be dealt with appropriately. If the communication breaches data protection legislation, this must be reported to the Data Protection Officer.

9.0 Personal and private use by staff

- 9.1 All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this access is not:
- 9.1.1 Taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)
 - 9.1.2 Interfering with the individual's work
 - 9.1.3 Relating to a personal business interest
 - 9.1.4 Involving the use of newsgroups, chat lines or similar social networking services
 - 9.1.5 At a cost to the School
 - 9.1.6 Detrimental to the education or welfare of pupils at the school
- 9.2 Excessive personal use of school facilities will likely be considered a disciplinary matter. It may lead to restricted access to computer equipment. Where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the staff member.
- 9.3 It is important for staff also to be aware that inappropriate use of their own personal or other ICT facilities in their personal time can have implications for their employment situation where this becomes known, and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.
- 9.4 Where school staff have brought their own personal equipment, such as mobile telephones, digital assistants, laptops and cameras, into the school, these personal items should not be used during pupil contact sessions unless authorised (smartwatches may be worn during these times, but not for personal use, e.g. text messaging). Staff should

follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these equipment pieces and that pupils do not access them at any time. Such personal equipment should not be used for school-related work (other than in an emergency). Where it is exceptionally so used, any materials produced/stored on this equipment must be transferred (if retention is necessary) securely and at the first opportunity to school equipment and then deleted from the staff's personal equipment.

- 9.5 Whilst individuals may be required to use their personal mobile telephone to contact the school, staff should exercise care and seek reimbursement as outlined in section 3.

10.0 Security and confidentiality

- 10.1 Any concerns about the security of the ICT system should be raised with a senior leadership team member.
- 10.2 Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.
- 10.3 School staff must consider any advice regarding what is permitted in downloading educational and professional material to the school server. When staff are provided with a memory stick for such activity, this should be used only to keep the material for the short term and then removed. All staff must review the appropriateness of the material before downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's ICT lead.
- 10.4 When working from home, staff should use their "ubikey" to work remotely or save documents containing personal data on an encrypted memory stick. When using their own devices, they must ensure that they have undertaken appropriate virus checking and materials are dealt with in accordance with 9.4 above to ensure that there is no breach of the school's Data Protection Policy.
- 10.5 Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system and/or VLE.
- 10.6 Whilst any school staff members may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.
- 10.7 The Business Manager will direct the school's network manager (Harrap) to ensure that all equipment is regularly updated with new software, including virus packages and that licences are maintained on all school-based and school-issued equipment. Staff must ensure they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.
- 10.8 Staff must ensure that their use of the school's ICT facilities does not compromise the rights of any individuals under the General Data Protection Regulations and the school's

Data Protection Policy. This is particularly important when using data offsite, and electronic data must only be taken offsite securely using an encrypted memory stick. In particular when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure they have the correct email address and verify the identity of the person they communicate the data with.

- 10.9 Staff must also ensure that they do not compromise any rights of individuals and companies under the copyright laws through their use of ICT facilities.

11.0 Monitoring

- 11.1 The school uses Harrap's ICT services and must comply with their email, internet and intranet policies.

- 11.2 The school and county council reserve the right to monitor the use of email, internet and intranet communications and, where necessary, data may be accessed or intercepted in the following circumstances:

- 11.2.1 To ensure that the security of the school and county council's hardware, software, networks and systems are not compromised.

- 11.2.2 To prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems.

- 11.2.3 To gain access to communications where necessary where a user is absent from work.

- 11.3 Where staff have access to the internet during their work, it is important for them to be aware that the school or county council may track the history of the internet sites that have been visited.

- 11.4 To protect the right to privacy, any interception of personal and private communications will not occur unless grounds exist to show evidence of crime or other unlawful or unauthorised use. Such interception and access will only occur following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

12.0 Whistleblowing and Cyberbullying

- 12.1 Staff concerned about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. Any matter concerning child safety should also be reported to the Designated Safeguarding Leader.

- 12.2 It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding E-Safety of the school staff. Staff are strongly advised to notify their

Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support Line (02380 626606[5]) and via the UK Safer Internet Centre helpline@safetinternet.org.uk or 0844 381 4772

13.0 Signature

- 13.1 School staff are required to read and sign a declaration as outlined in Appendix 1, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.
- 13.2 Staff must comply with the terms of this policy. Any breach will be considered a breach of disciplinary rules (such as the Staff Code of Conduct), which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.

Other School Policies

This policy should be read in conjunction with other school policies, including Child Protection, Anti Bullying, Behaviour, Confidentiality, Whistle Blowing, Equality, E-Safety, Mobile Phone, and Data Protection policies.

To ensure that staff members are fully aware of their professional responsibilities when using information systems and communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the details of the school's Policy for Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of systems, including cloud-based software, large language models, and authorized generative AI interfaces, mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking. ICT use may also include personal ICT devices when used for school business.
- I understand that using the school ICT system for a purpose not permitted may be a criminal offence.
- I will only use AI tools that have been formally approved by school leadership and backed by a verified DPIA (e.g., Microsoft 365 Copilot, Arbot)
- I will never upload identifiable pupil records, sensitive personal data, or special category information into unauthorized AI systems.
- I will critically verify all AI-generated teaching resources, data summaries, or report drafts for accuracy, potential bias, or algorithmic hallucinations before deployment, recognizing that I remain fully accountable for the content.
- I will respect the intellectual property of our pupils and ensure their academic or creative work is never used to train commercial AI networks without explicit parental consent.
- I understand that I cannot communicate confidential information to the school or that I do not have the authority to share and/or would be in breach of the General Data Protection regulations and the School's Data Protection Policy for me to hold or share.
- I understand that school information systems and hardware may not be used for personal or private use without the permission of the Headteacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using various methods of communication.
- I understand that I must not use the school ICT system to access inappropriate content.
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing, or bullying is an inappropriate use of ICT.
- I will respect system security and not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.

- I will follow the school's policy regarding downloading and uploading information and material.
- I will ensure that personal data is stored securely and used appropriately, whether in school, taken off the premises, or accessed remotely. I will not routinely keep personal data on removable storage devices. Where it is necessary to store personal data on a personal/removal storage device, I will ensure that it is password-protected and/or stored on an encrypted device. If the material needs to be retained (and can be retained per the school's Data Protection Policy), I will ensure it is transferred to secure school-based devices immediately after use and that it is deleted promptly from the removal storage device.
- I will respect copyright, intellectual property and data protection rights.
- I understand that using school equipment and/or accessing school internet for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Leader or Headteacher
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher or, if appropriate, the Chair of Governors.
- I will report any potential data breaches to the school's Data Protection Officer.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging, is compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.
- I understand the school's stance on the use of social networking and, given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote E-Safety with pupils in my care and help them to develop a responsible attitude to system use communication and publishing.
- I understand that inappropriate use of personal and other non-school-based ICT facilities can have implications for my employment at the school where this becomes known and that activities undertaken are inconsistent with expectations of staff working with children.

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images, or sound.

I have read and understand the Policy for Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from the Headteacher or Deputy Headteacher.

SIGNED:

Use of email, the internet, VLEs and school and HCC intranets

Do

- alert your Headteacher or designated manager if you receive inappropriate content via email
- be aware that the school's email system will be monitored and recorded to ensure policy compliance
- ensure that your email communications are compatible with your professional role
- give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate
- be aware that the school may intercept emails where it believes that there is inappropriate use
- seek support to block spam
- alert your Headteacher or designated manager if you accidentally access a website with inappropriate content
- be aware that a website log is recorded by the school and will be monitored to ensure policy compliance
- answer email messages from pupils and parents within your directed time
- mark personal emails by typing 'Personal/Private' within the subject header line

Don't

- send via email or download from email, any inappropriate content
- send messages that could be misinterpreted or misunderstood
- use personal email addresses to communicate with pupils or parents
- send messages in the heat of the moment
- send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude
- use email systems to communicate with parents or pupils unless approved to do so
- download attachments from emails without being sure of the security and content of the attachment
- forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention
- access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet
- upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging

Do

- Use authorized tools like Microsoft 365 Copilot as a creative starting point to save time on lesson planning, resource differentiation, and administrative drafting
-
- Thoroughly fact-check and edit all output to match the school's tone, values, and exact curriculum requirements
-
- Report any data security concerns, algorithm anomalies, or unexpected policy breaches to the Data Protection Officer immediately

Don't

- Use AI tools to replace human professional judgment in critical scenarios involving child safeguarding, student behavior tracking, or student admissions
- Feed sensitive internal school data, private communications, or confidential policy drafts into open, public AI search prompts
- Input names, addresses, or specialized special educational needs (SEN) tracking data into unauthorized tools

Use of telephones, mobile telephones and instant messaging

Do

- ensure that your communications are compatible with your professional role
- ensure that you comply with your school's policy on use of personal mobile telephones
- ensure that you reimburse your school for personal telephone calls as required
- use school mobile telephones when on educational visits

Don't

- send messages that could be misinterpreted or misunderstood
- excessively use the school's telephone system for personal calls
- use personal or school mobile telephones when driving
- use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do

- ensure that material recorded is for educational purposes only
- ensure that where recording equipment is to be used, approval has been given to do so
- ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy
- ensure that parental consent has been given before you take pictures of school pupils

Don't

- bring personal recording equipment into school without the prior approval of the Headteacher
- inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
- put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff

Use of social networking sites

Do

- ensure that you understand how any site you use operates and therefore the risks associated with using the site
- familiarise yourself with the processes for reporting misuse of the site
- consider carefully who you accept as friends on a social networking site
- report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site
- take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain
- ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page
- follow school procedures for contacting parents and/or pupils
- only contact pupils and/or parents via school based computer systems
- through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)