Hollywater School

Inspire. Believe. Achieve.

Acceptable Use of IT Policy

Approved by Chair of Governors: Silas Jones		**Date of approval:** July 2025
Headteacher: Sarah Kitching		
Date of last review:	14/05/2024	
Frequency of review ANNUAL and next review:	July 2026	

1. Introduction

This policy has been based on the Hampshire Model Policy for Staff Acceptable Use of ICT and should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- E-Safety Policy
- Safeguarding Policy
- Data Protection Policy

Staff are given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. Staff complete training throughout the year that focuses on how to keep themselves and pupils safe online.

2. Application

This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

This policy applies in respect of all IT resources and equipment within the school and resources that have been made available to staff for working at home. IT resources and equipment include computer resources, use of school internet access and email systems, software (including use of software such as SAP and SIMS), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work. This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal IT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

3. Access

School staff will be provided with a log on where they are entitled to use the school IT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

Access to certain software packages and systems (e.g. HCC intranet; SAP (HR, finance and procurement system), Arbor, remote access) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

Some staff may be provided with laptops, ipads and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is password protected and not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required

for updating of software, licences and virus protection. Termly checks are conducted on any school equipment to enable us to update software as necessary and carry out safeguarding checks.

Where the school provides digital cameras and other recording 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 consent has been provided by parents.

School mobile phones must be used during off site visits. In some cases, personal mobile phones may be used but this must be agreed by the Headteacher in advance. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

4. Communication with parents, pupils and governors

The school communicates with parents and governors through a variety of mechanisms – email, texts or home link books.

School must indicate to staff if any other staff are permitted to make contact using the systems below:

School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a class teacher where they feel they need to make a telephone call to a parent.

Text System – Admin staff. Where, in exceptional circumstances other staff need to send a text, this is normally approved by the Headteacher or delegated to a member of the Senior Leadership Team.

Letters – Normally all teachers may send letters home, but they must be approved by the Headteacher / Deputy Head before sending. Where office staff send letters home these will normally require approval by the Headteacher/Deputy Head.

Email – school email accounts should not routinely be used for communication with parents outside school hours. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Headteacher.

Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email.

5. Social Media

School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children.

Staff should make appropriate use of 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.

Staff should refer to the E-Safety Policy which contains detailed advice on the expectations of staff when using social media.

6. Unacceptable Use

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

- To communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share

- To present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others

- To access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material

- To communicate anything via IT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally.

- To communicate anything via IT resources that breaches the protected characteristics of an individual or group,

- To communicate anything via IT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils

- To upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment

- To collect or store personal information about others without direct reference to GDPR.

- To use the school's facilities and / or equipment, to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project.

- To use the school's facilities and /or equipment, 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.

- To undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children, young people and vulnerable young adults.

Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of IT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or IT lead.

Where an individual accidently accesses a website or material that they consider to be pornographic or offensive, this should be reported immediately to the Headteacher or other member of the Senior Leadership Team.

Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or Senior Leadership Team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material.

Genuine mistakes and accidents will not be treated as a breach of this policy.

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 member of the Senior Leadership Team so that this can be dealt with appropriately.

7. Personal and private use

All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

- Taking place at the expense of contracted working hours (i.e. is not taking place during paid working time.)
- Interfering with the individual's work.
- Related to a personal business interest.
- Involving the use of news groups, chat lines or similar social networking services.
- At a cost to the school.
- Detrimental to the education or welfare of pupils at the school.

Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

It is important for staff to also be aware that inappropriate use of their own personal or other IT 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.

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. 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 pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

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

8. Security and confidentiality

Any concerns about the security of the IT system should be raised with the Headteacher and/ or a member of the Senior Leadership Team.

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.

School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with a memory stick for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to 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 IT lead.

Where provided, staff should normally use their school issued laptop for remote access working. All remote work must be undertaken using the remote school network and work should be saved to the school network.

Staff are not permitted to use memory pens or memory sticks in school unless they are school issued and encrypted.

In exceptional circumstances e,g Subject Access Requests (SAR) and where encrypted files are too big for email, The Headteacher or Deputy Headteacher (as GDPR Officer), will authorise the use of a password secured school issued memory stick for these files. Transfer of these memory sticks will be via Special Delivery postage or by Hand.

Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil IT system.

Whilst any members of school staff 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.

The school will nominate staff who are responsible for ensuring 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 that they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.

Staff must ensure that their use of the school's IT facilities does not compromise rights of any individuals under GDPR. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of IT facilities.

9. Monitoring

The school uses Hampshire and Agile IT services and therefore is required to comply with their policies.

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:

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

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

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

Where staff have access to the internet during the course of 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.

To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place 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.

10. Whistleblowing and cyberbullying

Staff who have concerns about any abuse or inappropriate use of IT resources, virtual learning environments, camera/recording equipment, telephones, 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. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

It is recognised that increased use of IT has led to cyberbullying and/or concerns regarding e-safety of 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) and also via the UK Safer Internet Centre helpline@safetinternet.org.uk or 0844 381 4772

Further advice on cyberbullying and harassment can be found in the E-Safety Policy.

11. Remote Access

Hollywater School provides remote access to help support employees with the delivery of the curriculum and for teaching and learning. It is also intended for managing and administering the ICT networks.

Use of the school's remote access service implies acceptance of the conditions of use. The school may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

Uses of Remote Access Services

The following list is not exhaustive, but sets out broad areas which the school considers to be acceptable use of remote access:

- To gain access to School Information Management System (Arbor).
- To gain access to resources, files and software on the school network. To administer the school network remotely.

Any computer used to access the school's remote systems must possess anti-virus and anti-spyware programs. These must be updated regularly, at least once a week. The school bears no responsibility if use of the remote access system causes system crashes, or complete or partial data loss on connected computers. Users of remote access are solely responsible for backing up all data before accessing the system. At its discretion, the school will disallow remote access for any computer that proves incapable, for any reason, of working correctly with the remote access system.

When a computer is directly connected to the internet it can be contacted by any other computer also connected to the internet. As a result, there is a risk of exposure to malware that could connect to and potentially compromise that computer, which in turn risks infecting the school's system. For this reason, precautions must be taken to minimise this risk:

- Make sure up-to-date anti-virus software is installed.
- Make sure the latest operating system patches are installed.
- Run a weekly virus scan.
- If a computer has become infected with a virus or other malware, do not use it to remotely access the school's network until the virus has been deleted.
- Turn on phishing filters on web browsers to reduce the risk of phishing attacks.

- Use an anti-spyware program to detect spyware.

To avoid a risk of confidential information being disclosed to unauthorised third parties:

- Logout of remote access before leaving the computer.
- Wireless network connections must be encrypted using WPA2 or use a cable connection.
- Do not allow any unauthorised person, including family and friends, to use the remote access login or to access files held on the school's network.
- Use a password protected screensaver to prevent anyone gaining access to the computer
- Do not use password storing facilities found in some programs to automatically remember passwords.
- Do not reveal passwords. If for any reason a password is revealed this should be changed immediately.

This policy will ensure that staff are able to access the school network remotely without risk to the security of the system.

12. Signature

It will be normal practice for staff 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.

Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to IT facilities. Staff should be aware, that in certain instances, inappropriate use of IT may become a matter for police or social care investigations.

Hollywater School

Inspire. Believe. Achieve.

Appendix 1 Staff Code of Conduct for IT

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

- I appreciate that IT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC / Agile intranet access and use of social networking and that IT use may also include personal IT devices when used for school business
- I understand that it may be a criminal offence to use the school IT system for a purpose not permitted
- I understand that I am unable to communicate information which is confidential to the school or which I do not have the authority to 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 the various methods of communication
- I understand that I must not use the school IT system to access inappropriate content
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of IT
- I will respect system security and I will 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 in respect of downloading and uploading of information and material
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights
- I understand use 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 Lead (DSL) or Headteacher.
- I will report any incidences of inappropriate use or abuse of IT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are 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 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 any 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 IT 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 IT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's IT 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 Staff 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 IT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: …… DATE: ……

NAME (PRINT):

…….....