Policies

ICT & Internet Acceptable Use Policy

Next review date: November 2027



Contents

Contents 2

1. Introduction and aims 3

2. Relevant legislation and guidance 4

3. Definitions 5

4. Unacceptable use 6

5. Monitoring of school network and use of ICT facilities 8

6. Staff (including governors, volunteers, and contractors) 9

7. Students 12

8. Parents 13

9. Data security 14

10. Internet access 16

11. Artificial Intelligence 18

12. Monitoring and review 19

13. Related policies 20

Appendix 21

Appendix 1: Acceptable use of the internet: agreement for parents and carers 21

Appendix 2: Acceptable use agreement for students 22

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors 23

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for students, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching students safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our staff disciplinary policy or student behaviour policy.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- UK GDPR
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools
- DfE Filtering and Monitoring Standards

3. Definitions

- **“ICT facilities”:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **“Users”:** anyone authorised by the school to use the ICT facilities, including governors, staff, students, volunteers, contractors and visitors
- **“Personal use”:** any use or activity not directly related to the users’ employment, study or purpose
- **“Authorised personnel”:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **“Materials”:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Senior Leadership Team or Strategic ICT Manager will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the executive headteacher's discretion.

Requests for approval should be submitted via email to the executive headteacher.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour and staff discipline.

The behaviour policy can be found on the school's website under 'Key Information' > 'Policies'. The staff disciplinary policy can be found on the All Staff shared Google drive under 'Policies' > 'HR'.

5. Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT or safeguarding staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Safeguard our students and staff
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

5.1 Filtering and Monitoring Compliance (KCSIE & DfE Standards)

- In accordance with statutory guidance (*Keeping Children Safe in Education*) and the DfE's *Meeting digital and technology standards in schools and colleges*, the school implements appropriate, age-specific filtering and monitoring systems across all school-owned devices and networks.
- Roles & Governance:
    - The Designated Safeguarding Lead (DSL) maintains lead responsibility for overseeing filtering and monitoring systems, in partnership with the Strategic ICT Manager and the Director of Operations.
    - The Governing Board receives regular reports on the effectiveness of filtering and monitoring provisions and ensures annual reviews are conducted.
- Scope of Monitoring: Monitoring covers active internet traffic, web searches, email, device logs, and system logins. The school's system is configured to flag and report:
    - Child Sexual Exploitation and Abuse (CSAE / CSAM)
    - Radicalisation and extremism content (Prevent duty)
    - Self-harm and suicide-related searches
    - Bullying, hate speech, and harassment
- Breaches and Alerts: Any alerts triggered by serious safeguarding concerns will be escalated directly to the DSL or Deputy DSL without delay.

6. Staff (including governors, volunteers, and contractors)

6.1 Access to school ICT facilities and materials

The school's ICT support team manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Email
- The schools MIS
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and temporary passwords that they must use when accessing the school's ICT facilities. Temporary passwords must be changed to something more secure and 2 factor authentication must be set up when available.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT support team.

These requests should be submitted via email to the ICT support team.

6.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and students, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Data Protection Office or Senior Business Manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students. Staff may use the 3CX or Tripaid apps on their personal devices when on trips. These apps protect personal phone numbers while still allowing communication with parents and students.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

The school can record in-coming and out-going phone conversations. If a call is going to be recorded the caller MUST be made aware of this and the reason for the conversation being recorded.

Examples of when a conversation maybe recorded include (but are not limited to):

- To aid staff training
- Discussing a complaint raised by a parent/carer or member of the public
- If a member of staff feels threatened by a caller
- Discussing requests for term-time holidays
- Taking advice from relevant professionals regarding safeguarding, special educational needs assessments, etc.

Recordings will be stored in line with the school's data protection policy which can be accessed on the school's website.

6.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Strategic ICT Manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's e-safety policy which can be accessed on the school's website.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where students and parents could see them.

Staff should take care to follow the school's guidelines on social media and use of email (see section 6.1.1) to protect themselves online and avoid compromising their professional integrity.

6.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see the All Staff shared drive on Google under 'Staff Handbook').

6.3 School social media accounts

The school has an official Facebook, Instagram and a number of X (formerly Twitter) pages (https://www.hccs1978.co.uk/social-media-feeds), managed by the ICT Support Team and updated by nominated members of staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

7. Students

7.1 Access to ICT facilities

- Computers and equipment within the school are available to students only under the supervision of staff
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff
- Students will be provided with a Google account for email, drive storage and classroom which can be accessed from any device.
- Students will be provided with a student portal account to access homework, attendance and behaviour information which can be accessed from any device.
- Sixth-form students can use the computers in the study area independently for educational purposes only

7.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

7.3 Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the behaviour policy, if a student engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other students, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

8. Parents

8.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Parents may also be given access to the school's ICT facilities in order to give training on how to access relevant systems such as those for homework/behaviour etc.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

8.2 Communicating with or about the school online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 1.

9. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, students, parents and others who use the school's ICT facilities should use safe computing practices at all times.

9.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. We recommend following the advice from the NCSC for using 3 random words to generate your passwords:
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

Passwords should be unique for each different service that a user accesses.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Staff are required to use 2 factor authentication on all accounts where it is available. The ICT support team can provide instructions on how to do this. While this is not a requirement for students or parents we would always advise that 2 factor authentication is used to provide an extra layer of security on your accounts.

9.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

9.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

The school's data protection policy can be found on the school's website under 'Key Information' then 'Policies'

9.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the ICT support team.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT support team immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

9.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data or work remotely if they are accessing the data through cloud systems. Sync clients should not be used to download data to a personal device. Personal data must never be stored directly on personal devices unless authorised to do so by the executive headteacher.

Use of personal devices to store personal data will only be authorised if there is no other option and the devices have appropriate levels of security and encryption, as defined by the Strategic ICT Manager.

10. Internet access

All computers in the school provide a secure and filtered connection to the internet. The school's wireless networks also provide access to the same secure filtered connection.

- The school uses a filter to attempt to restrict access to inappropriate or dangerous websites.
- The school has a number of wireless networks to separate staff, students and visitors. The ICT support team will connect devices to these networks at their discretion.

Please note that while our internet connections are filtered we cannot always guarantee that inappropriate sites cannot be accessed. The school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the internet facilities.

If any member of the school community finds a site that they believe to be inappropriate they should immediately exit the site and report it to the schools ICT support team.

10.1 Students

HCCS Students will be allowed access to the school's wireless networks. When connecting to the guest networks students will be required to enter their school network credentials to ensure the appropriate level of filtering and monitoring.

- Wifi access is available in all buildings across the school site
- All connections to the wireless networks are monitored and filtered
- All students are permitted to access the wireless network but by doing so they agree that their internet use will be monitored for the duration of the connection.
- If a student has problems accessing the wireless network they should bring their device to the ICT support team. (We cannot guarantee that all devices will work)

10.2 Staff

HCCS Staff will be allowed access to the school's wireless networks. Staff can connect by entering their network credentials or by bringing their device to the ICT support team who can enter the password for them.

- Wifi access is available in all buildings across the school site
- All connections to the wireless networks are monitored and filtered
- All staff are permitted to access the wireless network but by doing so they agree that their internet use will be monitored for the duration of the connection.
- If a member of staff has problems accessing the wireless network they should bring their device to the ICT support team. (We cannot guarantee that all devices will work)

10.3 Parents, trainees and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the executive headteacher or ICT support team.

Authorisation will only be granted if:

- Parents are working with the school in an official capacity (e.g. as a volunteer)
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Internet access is required for training purposes in our onsite training facilities.

The wifi password will not be disclosed to anyone outside the ICT support team to ensure the security of the networks. In order to connect devices to the wireless network a member of the ICT support team will need to access the device to enter the required credentials.

11. Artificial Intelligence (AI)

All ll members of the school community must ensure that any use of generative AI aligns with the school's dedicated AI Policy. This policy is available on the schools website.
https://www.hccs1978.co.uk/policies-and-procedures

- Approved School Accounts (e.g. Gemini via Google Workspace for Education): When using enterprise AI tools provided under the school's managed domain, personal data should only be processed where strictly necessary for educational or operational purposes, and principles of data minimisation (e.g., pseudonymisation, removing unnecessary identifiers) must be applied.

- Public and Personal Third-Party AI Tools: Staff and students must never input personal, sensitive, confidential, or safeguarding data into free, consumer, or unapproved AI platforms, as these lack the school's data protection and privacy safeguards.

12. Monitoring and review

The Senior Business Manager and Strategic ICT manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year in line with KCSIE and DfE Filtering and Monitoring Standards.

The governing board is responsible for approving this policy.

13. Related policies

This policy should be read alongside the school's policies on:

- E-Safety
- Safeguarding and child protection
- Behaviour
- Staff disciplinary policy and procedures
- Data protection & Freedom of Information

All policies can be found either on the school's website under 'Key Information' > 'Policies' or alternatively on the All Staff shared drive on Google under 'Policies'.

Appendix

Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: ● Our official Facebook page ● Email/text groups for parents (for school announcements and information) ● Our virtual learning platform Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: ● Be respectful towards members of staff, and the school, at all times ● Be respectful of other parents/carers and children ● Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: ● Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way ● Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident ● Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Appendix 2: Acceptable use agreement for students

Acceptable use of the school's ICT facilities and internet: agreement for students and parents/carers	
Name of student:	
When using the school's ICT facilities and accessing the internet in school, I will not: ● Use them for a non-educational purpose ● Use them without a teacher being present, or without a teacher's permission ● Use them to break school rules ● Access any inappropriate websites ● Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) ● Use chat rooms ● Open any attachments, or follow any links in unsolicited, suspicious or unexpected emails, without first checking with a teacher ● Use any inappropriate language when communicating online, including in emails ● Share my password with others or log in to the school's network using someone else's details ● Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation ● Access personal social networking sites or chat rooms during teaching hours, in the presence of students, or using school equipment without prior authorisation from the Strategic ICT Manager. ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Share confidential information about the school, its students or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and Strategic ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**