Hinchingbrooke School

Hard Work   High Standards   Kindness

Policy Statement

on

INFORMATION
AND COMMUNICATION TECHNOLOGY
ACCEPTABLE USE FOR STUDENTS
(AUP)

Revised:	3 Yearly
Date approved by Governing Body:	October 2023

ICT Acceptable Use Policy

To make use of the School Network, Internet and e-mail access, students must read, sign and return the agreement for ICT Acceptable Use attached. Returns should be taken to the student's School Office.

The School has provided computer facilities and other technology for use by students, offering access to a vast amount of information for use in studies. The computers are provided and maintained for the benefit of all students, and you are encouraged to use and enjoy these resources and help to ensure they remain available to all. Students are responsible for good behaviour with the resources and when using the Internet. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

If **British decency laws** or the **Computer Misuse Act 1990** is breached then a student may have the matter referred to other authorities including the Police. The Computer Misuse Act 1990 that is upheld at Hinchingbrooke School includes:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computers
4. Unauthorised acts causing, or creating risk of serious damage.
5. Making, supplying or obtaining articles for use in an offence under these sections.

Listed below are the conditions of the student ICT AUP agreement. If any student breaks these provisions, access to the Network, Internet and Email will be refused and the student will be subject to formal action.

Terms and Conditions of this Agreement

1. Personal Responsibility
As a student of the school, I will ensure that any misuse of the network is reported to a staff member. Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence and attempts to disrupt or hack into the school's network.

2. Acceptable Use
The use of ICT must be for the purpose of education and in accordance with the ethos and values of Hinchingbrooke School. Students are personally responsible for ensuring that they are correctly using the school network under this condition.

The sending and sharing of any material that breaks any United Kingdom or other national laws is prohibited. This includes **copyrighted material**, threatening or obscene material or material protected by trade laws.

The School's networking facilities are not to be used for the buying or selling of goods. This includes access gained from the wireless network.

3. Privileges
The use of the ICT is a privilege and inappropriate use can result in that privilege being withdrawn. Students will receive regular updates on the appropriate use of IT facilities within their lessons. Hinchingbrooke School staff will make decisions on what is considered appropriate use if a case of misuse is raised by staff or students.

4. Vandalism
Vandalism is defined as any malicious attempt to harm or destroy any:
- School ICT equipment
- Data of another student
- Data on the School network.

This would include uploading or creating computer viruses, damaging computer hardware or deleting data from where it is stored.

5. Email
Email is provided by the school through Office 365 Outlook accounts. Sending or receiving any email, which contains inappropriate material, is strictly forbidden. This material may include pornography, unethical or illegal requests, racism, sexism, inappropriate language, or material that may cause offence to others. Formal action will be taken in all cases. It is also forbidden to send large volume emails to others (spamming). Email is not guaranteed to be private. Messages relating to illegal activities may be reported to the Police.

6. Internet Search Engines
Students are required to use Internet search engines responsibly and under the guidelines of classroom teachers. If students are found to be searching for unsuitable material they will face formal action. Inappropriate Internet searching is logged by the School's Sophos filtering programme and monitored by IT Technicians.

Students are strictly forbidden from tampering with safety filters from Internet Search engines.

7. Network Etiquette
Students are expected to follow general rules of politeness and respect whilst using the School's IT equipment. These rules include the following:

  a.   **Be polite**. Never send abusive messages of any form to other people. Follow school guidelines on netiquette. Communicate as if speaking to somebody face-to-face.

  b.   **Use appropriate language**. Never swear, use any other inappropriate or offensive language. Consider that your teacher is reading over your shoulder when you are typing.

  c.   **Personal details**. Never reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other students.

  d.   **Password**. Never reveal your password to anyone. If you think your password has become compromised, contact an IT Technician immediately.

  e.   **E-Safety**. Ensure that you are making reasonable steps to protect yourself online from cyberbully attacks and trolling.

  f.   **Other considerations**:
    - Use references for any research you use. Do not copy another person's work and pretend that it is your own. This is called **plagiarism**. This is particularly important when submitting coursework and controlled assessment work.
    - Remember that humour is very often misunderstood when sent electronically.
    - Although you may be alone on your PC, all activities you carry out can be traced back to you.
    - Respect the rights and beliefs of others.

8. Chat Services
Students are not permitted to use Internet chat services whilst on the School network. This is to protect students from exposure to the potential risk of unknown chat users.

9. Services
Whilst making every effort to do so, Hinchingbrooke School makes no guarantees of uninterrupted network service provision. Hinchingbrooke School will not be responsible for the loss or damage of any data stored on our network system. Use of any information collected using the network or other IT systems is at the students own risk.

Students should be aware that network storage is not infinite and appropriate use of storage must be observed. Students should regularly manage their files stored on the school network and delete, archive or relocate data to an alternative location, such as One Drive in Officer 365.

10. Connected Devices
During the time that any removable device is attached to an item of the School network, it becomes part of that system and so is subject to the same restrictions as any other device previously identified.

Students are not permitted to tamper with any connected devices such as keyboards, mice, monitors and power cables. If there is a problem with the hardware, speak to a teacher or contact an IT Technician.

11. Security
Security on Hinchingbrooke School's network and services is set at a high standard to protect all users. If you notice a security concern, inform an IT Technician at once. Your use of the system must always be under your own username and password. Remember to keep your passwords secret. Do not share them with friends as you are putting your own user account at risk. Anyone caught sharing passwords or using other student login details may have their privileges removed and be subject to formal action.

12. Bring Your Own Device (BYOD)
Students choosing to connect their personal devices to the school's wireless network accept that they must comply with the requirements and terms of this policy and abide by the **ICT Bring Your Own Device (BYOD)** policy.

ICT Acceptable Use Policy for Students

Student User Agreement

It is most important that you read over the document before you sign and return the form to your School Office.
Please retain your copy of the ICT Acceptable Use Policy for your records.

For the Student:

I understand and agree to adhere to the conditions of the ICT Acceptable Use Policy. I understand that if I fail to follow these guidelines, I am likely to be subject to disciplinary action by Hinchingbrooke School. I understand that I am a member of the school community and as such have a responsibility to report any signs of misuse to the IT Technicians. I understand that Hinchingbrooke School has a duty to protect the E-Safety of all students under these guidelines.

Student Name: _____

Student Signature: _____

Form Group: _____

For the Parent/Carer:

As a parent/carer, I have read and understood the ICT Acceptable Use Policy. I have taken the time to discuss this with my son/daughter and support Hinchingbrooke School's steps towards providing safe use of IT systems in school. I understand that although the school has a filtering system for Internet use, it is impossible to restrict access to all controversial materials that may be sourced using the School's IT systems.

Parent/Carer Name: _____

Signature: _____

Date: _____

For Office use only
Date received:
Added to file: