Acceptable Use of ICT Policy - Students (Approved Spring 2026)

Status	Non Statutory	**Date created**	September 2021
Any other statutory names for this policy (where applicable)		**Date first approved**	December 2021
Responsibility for this policy (job title)	Deputy Headteacher	**Date last reviewed**	Approved Spring 2026
Governors' Committee with responsibility for its review	Teaching & Learning	**Frequency of review**	Annual
Tick here if Bucks Policy attached in its entirety		**To be put on the school website?**	Yes
Approval necessary	Sub Committee		

Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), 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 pupils
- Establish clear expectations for the way pupils 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 pupils safe and effective internet and ICT use

Breaches of this policy may be dealt with under our Behaviour Matrix.

AHS seeks to implement this policy through adherence to the procedures set out in this document, and through commitment to staff and pupil training.

This policy should be read in conjunction with other school policies in the Governance & Policy page on our website:

- Behaviour and Exclusions Policy including Behaviour Matrix and Anti-Bullying Strategy
- Data Protection and Confidentiality Policy
- Child Protection and Safeguarding Policy
- Equality Statement
- AI policy
- Online Safety Policy

By using computers and digital tools at Aylesbury High School, students agree to abide by the following rules:

General Use of ICT Facilities

- You must not install programs or applications onto school devices, or bring software into school on external devices.
- You must not use school computers, chromebooks and digital tools for commercial purposes (e.g. buying or selling goods).
- School computers, chromebooks and digital tools must only be used for school-related activities and purposes in school.
- You may be liable to pay for damage caused to school owned devices by negligence or misuse.
- You must ensure passwords are kept confidential at all times. Passwords or accounts must not be shared with friends. If you suspect your account password has been compromised, please inform IT.
- You must abide by any rules or restrictions put in place for printing. All printing is monitored and printing privileges may be removed from students who abuse this facility.
- You must not attempt to alter or interfere with the configuration of school computers, chromebooks and digital tools.
- You must not attempt to access, copy or alter the work and files of other students or members of staff.
- You must show consideration for others when using school computers, chromebooks and digital tools and ensure that you do not harm, harass, offend or insult anyone.

Internet and Digital Use

- The internet must only be used for study purposes or school related activities.
- You must not use the internet to harm, harass, offend or insult anyone.
- You must not use the Internet to get, download, send, print or display any materials that are unlawful, obscene or abusive.
- You must respect the work and ownership of people outside the school, as well as other students and staff. This includes abiding by copyright laws.
- Use of chat rooms, forums and instant messaging apps is strictly prohibited in school.
- You must never share personal or sensitive information online, including: your full name, home address, telephone numbers, school name, pictures, photos or any other information that could be used to identify yourself or other students.
- You must be aware that all internet and email usage is monitored.
- The use of generative AI tools (such as ChatGPT) is generally not permitted on the school's systems or for the vast majority of homework tasks, unless a teacher explicitly sets a task allowing or instructing its use.
- You must adhere to the school's AI guidance for all AI-generated content, including proper attribution, acknowledgment, and transparency.
- You must not pass off AI-generated content as your own work; this is a form of plagiarism and constitutes academic misconduct.

These are not exhaustive lists. The school reserves the right to amend these lists at any time. The Finance & Operations Director will use professional judgement to determine whether any

act or behaviour not on the lists above are considered unacceptable use of the school's ICT facilities.

Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion. Applications for such exemption must be made in writing to the Headteacher.

Sanctions

By using computers at AHS, you realise and agree that access to the AHS computer network is a privilege, not a right and that this privilege may be revoked if these rules are broken. Sanctions will also be applied for misuse of AI, which is considered academic malpractice. Additional action may be taken by the school in line with existing practice regarding inappropriate behaviour and if appropriate, the police may be involved or other legal action taken.

Access to ICT facilities

The following ICT facilities are available to pupils, when instructed and supervised by the relevant member of staff:

- Computers and equipment in the school's ICT suites
- Specialist ICT equipment, such as that used for music, or design and technology

Pupils will be provided with an account linked to the school's Google Classroom, which they can access from any device, including their chromebooks, by using the following URL https://www.ahs.bucks.sch.uk/.

- Student and staff passwords should be a minimum of eight characters, including numbers and letters, and all users should consider changing their password at regular intervals, perhaps once a term.
- One should not use one's own name or username as a password, for example smith1
- One should not use one's password on anything you leave unattended
- All users must change their password immediately if they think someone has learned their password
- All users must remember that a school is a public place. They must always make sure they have completely logged off or locked the computer before leaving it unattended. Failure to do so will be considered a contravention of school policy. If an offence has been committed by some other person on their unattended computer, this may be considered as facilitating the Misuse of a Computer, which is a criminal offence

Sixth-form pupils can use the computers in the ICT suites, library or sixth form centre independently for educational purposes only.

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 pupils' 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.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Behaviour & Exclusions Policy, if a pupil 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
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, 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

Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Pupils who use the school's ICT facilities should use safe computing practices at all times.

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

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

Students who disclose account or password information may face disciplinary action.

Internet access

The school wireless internet connection is secured.

All students are given access to wifi whilst at school and this is in all areas of the school. In Y7-11 we do this through the use of Chrome Education Upgrades which are added to each student's Chromebook. In Y12-13 our students are given codes for the BYOD network and can access wifi this way.The Chrome Education Upgrade gives our IT team more control of what users access. It also allows for updates and apps to be pushed out to all users. All students using the school wifi are subject to the Smoothwall filtering that the school subscribes to. Additionally, we make use of Securly which allows teachers to see the screens of the students in their class and Smoothwall Monitor which alerts the DSL team to concerning activity from students.

Commitment

Students

- I will follow the Acceptable Use Policy above
- will follow the school's AI guidance at all times, including the rules regarding when and how AI can be used for homework and assessments.
- will adhere to school guidance for using AI-generated content, including proper attribution and respect to creators
- will never input Intellectual Property or Personal and Sensitive data into AI tools
- understand that misuse of AI, including passing off AI-generated content as my own work, constitutes malpractice and will be sanctioned.

Parents

- will support the Acceptable Use Policy above
- will support their child in understanding Intellectual Property rights and responsibilities related to AI-generated content
- will ensure their child complies with school policies (such as the AI Guide for Students) regarding AI-generated content, including proper attribution and ethical use.
- will support the school's policy on AI use and understand the implications of academic misconduct (malpractice) for their child's examinations and future conduct.

Monitoring and review

The DHT will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year. The Teaching and Learning Committee of the Governing Board is responsible for approving this policy.