Acceptable Use of ICT Policy - Students

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**	December 2021
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		

1. 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.

2. Relevant legislation and guidance

This Policy applies to all computers fully or partially owned or operated by Aylesbury High School (AHS), and to any computer and mobile device used on its premises whether connected to the school network.

This includes:

- The voice and data networks that connect them
- All devices connected to these computers and networks
- All hardware and software associated with these systems
- The information managed by these systems

This Policy applies to all pupils of the School. It aims to ensure that all users are aware of how to use ICT responsibly and safely. AHS is fully committed to ensuring that the application of this policy is nondiscriminatory, in line with the UK Equality Act (2010).

This policy complies with the following legislation and guidance:

Data Protection Act 2018

The General Data Protection Regulation

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 2021

Searching, screening and confiscation: advice for schools

National Cyber Security Centre (NCSC)

Education and Training (Welfare of Children Act) 2021

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:

- Behaviour and Exclusions Policy eiht Behaviour Matrix and Anti-Bullying Strategy
- Data Protection and Confidentiality Policy
- Equality Statement
- Child Protection and Safeguarding Policy

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, pupils, 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

See appendix 1 for a glossary of cyber security terminology.

4. Unacceptable use

Pupils must be aware that:
All network activity is monitored and recorded.
All emails (even when deleted) and their history are logged and archived .
Members of the ICT staff may look at any files and communications to ensure that the system is being used responsibly and ICT staff can view your computer screen at any time, from anywhere on the school network without you knowing about it.

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
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- 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, its pupils, 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
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Deputy Head 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 (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.

4.2 Sanctions

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

5. Pupils

5.1 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 suite

- 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/ .

- Your password should be a minimum of eight characters, including numbers and letters, and consider changing your password at regular intervals, perhaps once a term.
- Do not use your own name or username as a password, for example smith1
- Do not write your password on anything you leave unattended
- If you think someone has learned your password, change it immediately
- Remember that a school is a public place. Always make sure that you 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 your 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.

5.2 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 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.

5.3 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

6. 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.

6.1 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.

7. 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 Smoothwall Classroom Manager 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.

10. Monitoring and review

The Deputy Head and ICT manager 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.

Appendix 1: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

term	definition
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.

Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's

	from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.