Alcester Academy

TO BE THE BEST THAT WE CAN BE

ICT and Internet Acceptable Use Policy

Author	**Leadership Team**
Approved by:	**Qu of Ed/HR Sub-Committee**
Reviewed by:	**Qu of Ed/HR Sub-Committee**
Last reviewed:	**March 2025**
Next review due by:	**3 Years – Autumn Term 2028**

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our Academy works, and is a critical resource for pupils,

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

This policy aims to:

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

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

Breaches of this policy may be dealt with under our "Staff Code of Conduct for all staff and volunteers" and the "Behaviour and Discipline Policy" for students.

2. Relevant legislation and guidance

This policy refers to, and 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 Academys
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

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 Academy to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"DPO":** Is the Academy designated Data Protection Officer.
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the Academy 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 6 for a glossary of cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the Academy's ICT facilities includes:

- Using the Academy's ICT facilities to breach intellectual property rights or copyright
- Using the Academy's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Academy'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 Academy, or risks bringing the Academy into disrepute
- Sharing confidential information, or images/videos about the Academy, its pupils, or other members of the Academy community
- Connecting any device to the Academy's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Academy'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, to any password-protected information, or Academy Social media Accounts without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Academy'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 Academy
- Using websites or mechanisms to bypass the Academy'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 Academy reserves the right to amend this list at any time. The Headteacher or Senior leader will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Academy's ICT facilities.

4.1 Exceptions from unacceptable use

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

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Academy's policies within the student Behaviour and Discipline Policy/Staff Code of Conduct.

Revoking permission to use the Academy's systems may also be applied.

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

5.1 Access to Academy ICT facilities and materials

The Academy's SLT, along with the ICT Support Lead manages access to the Academy's ICT facilities and materials for Academy staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programs, stored folders or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the Academy's ICT facilities.

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 their appropriate Line Manager/Senior Leader

Contacting ICT Support directly will lead to a polite refusal and trigger communication with the appropriate Line Manager/Senior Leader

5.1.1 Use of phones and email

The Academy provides each member of staff with two email addresses.

- These email accounts should be used for work purposes only. The Office365 Account is primarily for all administrative work and the google account for internal information, teaching and learning and student contact.

All work-related business should be conducted using the email addresses the Academy has provided.

Staff must not share their personal email addresses with parents and pupils, 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 that contains the personal information of another person, they must inform the DPO immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the Academy to conduct all work-related business.

Academy 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.

Special Circumstances:

Staff who would like to record a phone conversation should speak to the Headteacher or Senior Leader.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

For instance, you may grant requests to record conversations when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEND) assessments, etc.
- Discussing requests for term-time holidays

5.2 Personal use

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

Personal use is permitted provided that such use:

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

Staff may not use the Academy'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 Academy's ICT facilities for personal use may put personal communications within the scope of the Academy's ICT monitoring activities (see section 5.5). 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 Academy's ICT policy.

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

Staff should take care to follow the Academy's guidelines on social media and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.3 Remote access

We allow staff to access the Academy's ICT facilities and materials remotely.

Staff accessing the Academy's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the Academy's ICT facilities outside the Academy and take such precautions as the ICT Support Lead may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

5.4 Use of Staff Devices

All staff have been allocated a device, but it will remain the property of Alcester Academy and will returned to us when your contract has been completed.

5.4.1 Guidelines:

- When not in use it must be locked up or secured appropriately.
- It must never be left in an unattended vehicle.
- When it is being kept at your home, it must be kept out of sight (i.e. not where it could be viewed through a window).
- The device must never be taken abroad without prior consent from the Headteacher and insurance company if required.
- The school is not responsible for the purchase of peripheral devices (printers etc.), consumables or internet costs from home.
- The device should not be loaned to other individuals or Students (e.g., family members or friends).
- Staff are expected to abide by the school's "Acceptable Use Agreement" at all times when using the device – be it at home or at school.

If the above guidelines are known to be NOT followed, the staff member (or any personal home insurance) will be liable for replacement of the device if it is lost or stolen.

5.4.2 Returned Devices:

- must be returned to the Academy when instructed, in good condition.
- Staff must return the device to the school, upon any reasonable request for any reason. They will be given reasonable notice of this (At least 24hrs).
- In the event of a hardware or software problem, staff will not attempt to repair the device themselves or have it repaired by a third party. The device must be returned to the Academy which will take appropriate action.
- The academy expects staff to take good care of the device. If a repair is necessary due to negligence, the member of staff will be required to meet the cost of the repair.

5.5 Monitoring of Academy network and use of ICT facilities

The Academy reserves the right to monitor the use of its ICT facilities and network and maintains a safeguarding analysis system of all ICT network activity. This includes, but is not limited to, the monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Content, produced on all applications by all users
- User activity/access logs
- Any other electronic communications

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

The Academy monitors ICT use in order to:

- Obtain information related to Academy business
- Complete Safeguarding procedures, standards and protocols
- Investigate compliance with Academy policies, procedures and standards
- Ensure effective Academy 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

6. Pupils

6.1 Access to ICT facilities

All ICT facilities are available to pupils, under the following circumstances:

Computers and equipment in the Academy's ICT suite are available to pupils only under the supervision of staff

Specialist ICT equipment, such as that used by Performing Arts, Science or Design Technology, must only be used under the supervision of staff. For example, Vinyl Cutter, Digital Cameras, Mac Probooks or Data Loggers.

Pupils will be provided with an account linked to the Academy's virtual learning environment. This is in the form of Office 365 (@alcesteracademy.org.uk) and also Google Gsuite (@alcester.academy)

6.2 Search and deletion

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

The Academy 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 Academy'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.

6.3 Unacceptable use of ICT and the internet outside of Academy

The Academy will sanction pupils, in line with the Behaviour and Discipline Policy, if a pupil engages in any of the following **at any time** (even if they are not on Academy 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 Academy'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 Academy, or risks bringing the Academy into disrepute
- Sharing confidential information about the Academy, other pupils, or other members of the Academy 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 Academy'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

See the Behaviour and Discipline Policy for sanctions.

7. Parents

7.1 Access to ICT facilities and materials

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

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

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

7.2 Communicating with, or about the Academy online

We believe it is important to model for pupils, 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 Academy through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8. Data security

The Academy 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 Academy cannot guarantee security. Staff, pupils, parents and others who use the Academy's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the Academy'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.

Members of staff or pupils 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.

All staff must keep their passwords secure and may prefer to use a password manager app.

The Academy IT support team will generate passwords for pupils upon joining the Academy and the students will be forced to create their own password where this is necessary.

8.2 Software updates, firewalls and anti-virus software

All of the Academy'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 Academy's ICT facilities.

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

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Academy's Data Protection Policy.

Link: Google Drive\Shared Drives\Staff Information\Policies\Current Policies\Data Protection Policy.pdf

8.4 Access to facilities and materials

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

These access rights are managed by the appropriate Line Manager/Senior Leader, who is the designated keyholder.

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 appropriate Line Manager/Senior Leader 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.

8.5 Encryption

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

Academy staff may only use personal devices (including computers and USB drives) to access Academy data, work remotely, or take personal data (such as pupil information) out of Academy if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Strategic Lead.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The Academy will:

- Work with governors, Concero and the IT Strategic Lead to make sure cyber security is given the time and resources it needs to make the Academy secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the Academy's annual training window) on the basics of cyber security, including how to:
- Check the sender address in an email
- Respond to a request for bank details, personal information or login details
- Verify requests for payments or changes to information

- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents.
- Investigate whether our IT software needs updating or replacing to be more secure.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.
- Put controls in place that are:

- **'Proportionate'**: the Academy will verify this using a third-party audit annually, to objectively test that what we have good practice.
- **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
- **Up-to-date:** with a system in place to monitor when the Academy needs to update its software

Back up critical data automatically overnight each day, on and off site. Also store a weekly backup on an external hard drive that isn't permanently connected to the Academy network and safely stored away from the main server location.

- Delegate specific responsibility for maintaining the security and backup of our management information system (MIS) to our IT Service provider.
- Make sure staff:
- Connect to our network using a virtual private network (VPN) when working off site.
- Enable multi-factor authentication where they can, on things like Academy email accounts
- Store passwords securely using a password manager or Multi Protective File.
- Make sure ICT support staff conduct regular access reviews to make sure each user in the Academy has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Develop, review and test an incident response plan with the IT department, for example, including how the Academy will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access

The Academy wireless internet connection is secure. All channels are filtered at the student level of access.

All Staff and Students use the AHS4240 channel which is configured on all Academy devices with WiFi capability.

Visitors must obtain, from Reception, a Guest Voucher to connect their device to the GUEST channel.

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10.1 Pupils

Students can use Academy devices which are already configure for them to use.

The Academy will NOT allow students to access the Wifi on any private device except for those configured by the Academy IT technical team at the request of a Line Manager/Senior Leader.

For instance:

- A student has a specialist laptop/tablet with specific software to enable them to access their normal day to day lessons.
- A student is provided with a Laptop Loan Scheme device, promoted by the Academy.

10.2 Parents

Parents visiting the Academy will not be permitted to use the Academy's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the Academy in an official capacity (e.g. as a volunteer/member of a PTA)

10.3 Visitors

Visitors may need to access the Academy'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). Reception will be given authorisation to provide a Voucher by a Line Manager/Senior Leader.

Settings:

- The default duration is 8 hours
- The default length of time a voucher remains current is 7 days.
- The voucher use will be set to "One Time" only.

The Receptionists must receive in writing any changes that are required for a Guest, outside of the default settings and this can only be done by a Line Manager/Senior Leader.

11. Monitoring and review

The headteacher and the IT Strategic Lead monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Academy.

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

12. Related policies

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

- Online Safety
- Child Protection and Safeguarding
- Behaviour and Discipline
- Staff Code of Conduct
- Data Protection
- Remote Learning Risk Assessment
- The Acceptable Use Agreements

Appendix 1: Acceptable Use Agreements

Acceptable use agreement for pupils

Acceptable use of the Academy's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the Academy's ICT facilities and accessing the internet in Academy, 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 Academy 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 in emails, or follow any links in emails, without first checking with a teacher.

Use any inappropriate language when communicating online, including in emails

Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo .

Share my password with others or log in to the Academy's network using someone else's details.

Bully other people.

- I understand that the Academy will monitor the websites I visit and my use of the Academy'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 Academy's ICT systems and internet responsibly.

I understand that the Academy can discipline me if I do certain unacceptable things online, even if I'm not in the Academy when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the Academy's ICT systems and internet when appropriately supervised by a member of Academy staff. I agree to the conditions set out above for pupils using the Academy's ICT systems and internet, and for using personal electronic devices in Academy, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Acceptable use of the Academy's ICT facilities and the internet: agreement for staff and governors.

Staff/Governor Name:

Position:

When using the Academy's ICT facilities and accessing the internet in Academy, or outside Academy 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 Academy's reputation
- Access social networking sites or chat rooms
- 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 Academy's network
- Share my password with others or log in to the Academy's network using someone else's details
- Share confidential information about the Academy, its pupils 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 Academy

I understand that the Academy will monitor the websites I visit and my use of the Academy'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 Academy, and keep all data securely stored in accordance with this policy and the Academy's data protection policy.
- Any unexpected personal costs incurred through the use of Academy Technology will be charged directly to the staff member and action taken for inappropriate use. e. g. Academy issued mobile phones.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil 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 Academy's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
- I will respect copyright and intellectual property rights.

Signed (staff member/governor):	**Date:**

Acceptable use agreement for Visitors

This agreement has been drawn up to use alongside the new Visitors Wi-Fi system.

Users are identified by a register in the office kept by Reception alongside the Voucher Code. When the user accesses the Academy Wi-Fi, they can only proceed by accepting the following agreement.

Acceptable use of the Academy's ICT facilities and the internet: Agreement for Visitors

When using the Alcester Academy's ICT facilities and accessing the internet in or outside the main building on my 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 it in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- 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 pupils 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 and filter 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, and keep all data securely stored in accordance with this policy and the school's data protection policy.

Voucher Code:

Valid for:

Appendix 2: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the Academy 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.

TERM	DEFINITION
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.

Agreement for Use of a Student allocated Academy Laptop in School.

Alcester Academy defines a laptop computer as a portable microcomputer including electronic tablets and notepads. The purpose of these guidelines is to ensure that students recognize the limitations that the Academy imposes on the use of laptops for the purpose of safety and classroom integrity. In addition to these guidelines, the use of any computer in the Academy, including laptop computers, requires students to abide by the Academy's Pupil Acceptable Use Agreement which is available on the Academy's webpage.

A student allocated laptop is when a student continues to use a specific laptop in many lessons.

There are many benefits for a student to regularly use a laptop. There are also many areas of caution which need to be considered.

General Usage

Alcester Academy is providing the opportunity for the student to use a laptop as an educational tool to increase learning and achievement. The use of these laptops will be at the classroom teacher's discretion.

The student will:

1. use oa personalised laptop to support the instructional activities occurring in the classroom.
2. obtain teacher permission before using a laptop regularly in class.
3. use only their assigned and authorized laptop.
4. not "lend" their laptop to another student during a lesson without clear instruction and full co-operation of the teacher.
5. turn off and put away a laptop when requested by a teacher.
6. not use their laptop in areas of the Academy that are outside of the classroom.
7. have their laptop confiscated, subject to teacher discretion, if found in violation of this agreement.

Security

Alcester Academy recognises that the loss or damage of possessions can be a very upsetting and traumatic experience and we need to clearly set out the position of all concerned to hopefully minimise the impact of such an event and to clearly lay out the Academy's position, should this occur.

1. Security of the laptop/tablet is the sole responsibility of the student who needs to carefully look after the equipment and consider using an Alcester Academy lockable locker if they wish to leave the laptop while they move elsewhere.
2. Academy owned allocated laptops that are stolen or damaged are the responsibility of the student and their parents or guardians.
3. Leaving equipment with someone else in the Academy can be very tempting but not recommended. You are responsible for any loss or damage and Alcester Academy will not support any claims against a third party in such circumstances.
4. A protective purpose designed laptop bag is provided for extra protection. It is possible to purchase back packs with purpose designed laptop carriers which are less detectable.

You may be able to find insurance through your home insurance policy or as a separate insurance agreement for this use.

Fit for Purpose

1. The student laptop will have a full virus checker working and malware system in place.
2. The student will agree that there are no discomforting, indecent or inappropriate material or files on the laptop and agree to a random search as further evidence as such.

Network Security and Vulnerability

1. The Academy laptop **will** be configured to give full student access; the same as if using a workstation.

2. The student will be reminded of the terms and conditions of our 'Pupil ICT Acceptable Use Agreement' and this will be fully emphasised and agreed, completed by a signature of evidence that this process has been fulfilled.

You'll be aware that we cannot jeopardise our own IT system in any way. If there is any breakdown in our network system and the issues are tracked back to the student's laptop, we would have to look to you as parents to financially support this to be rectified. We are aware that the likelihood of this is extremely low, however it does need highlighting from the out-set.

Students and their parents/guardians wishing to take advantage of this programme must comply with all rules and regulations set forth in this agreement.

Agreement

By choosing to participate you are consenting to the monitoring and verification of use, and to examination of the student's laptop as set forth above.

All violations of the above procedures may result in the confiscation, loss of privileges, the

student's parents contacted, and any consequences outlined in the Academy's code of conduct.

We have reviewed these rules and regulations with my child.

Student Name _____

Student Signature _____

Parent/Guardian Name_____

Parent/Guardian Signature_____

Date_____

(A copy will be returned to you for reference purposes)

Agreement for Personal Use of Student-Owned Laptop in School

Alcester Academy defines a laptop computer as a portable microcomputer including electronic tablets and notepads. The purpose of these guidelines is to ensure that students recognize the limitations that the Academy imposes on the use of personal laptops in terms of classroom safety and integrity of use. In addition to these guidelines, the use of any computer in the Academy, including laptop computers, requires students to abide by the Academy's Pupil Acceptable Use Agreement which is available on the Academy's website.

There are many benefits for a student to use their own laptop. There are also many areas of caution which need to be considered.

General Usage

Alcester Academy is providing the opportunity for students to bring a personal laptop to school to use as an educational tool to increase learning and achievement. The use of these laptops will be at the classroom teacher's discretion.

The student will:

1. use a personal laptop to support the instructional activities occurring in the classroom.
2. obtain teacher permission before using a personal laptop regularly in class.
3. use only their personally owned authorised
4. not "lend" their laptop to another student during a lesson without clear instruction and full co-operation of the teacher.
5. turn off and put away a personal laptop when requested by a teacher.
6. not use their laptop in areas of the Academy that are outside of the classroom.
7. have their laptop confiscated, subject to teacher discretion, if found in violation of this agreement.

Security

Alcester Academy recognises that the loss or damage of personal possessions can be a very upsetting and traumatic experience and we need to clearly set out the position of all concerned to hopefully minimise the impact of such an event and to clearly lay out the Academy's position, should this occur.

1. Security of the laptop/tablet is the sole responsibility of the student, who needs to carefully look after the equipment and consider using an Alcester Academy lockable locker if they wish to leave the laptop while they move elsewhere.
2. Laptops that are stolen or damaged are the responsibility of the student and their parents or guardians.
3. Leaving your equipment with someone else can be very tempting but is not recommended. The student is responsible for it's loss or damage and Alcester Academy can not support any claims against a third party in such circumstances.

We recommend using a protective purpose designed laptop bag, it will provide extra protection. It is possible to purchase back packs with purpose designed laptop carriers which are less detectable. ***You may wish to consider finding insurance through your home insurance policy or as a separate insurance agreement for this use.***

Fit for Purpose

Before agreeing to the use of a student's laptop the IT Technical Support team will review the configuration and setup of the laptop.

1. The student will be able to demonstrate to the Academy that the laptop has a full virus checker working and malware system in place.
2. The student will agree that there are no discomforting, indecent or inappropriate material or files on the laptop and agree to a random search as further evidence as such.
3. The student will show a full list of internet browser favourites and links and recognise any links which will infringe the Acceptable Use Agreement, stating that these will not be used within the Academy.

Please note: The Academy IT personnel will not be responsible for fixing, repairing, or downloading programs to student laptops if there is a problem with their laptop.

Network Security and Vulnerability

1. The laptop **will not** be configured to give full student access (unlike normal log on to our network), but the user will have access by using our student filtered wi-fi system and access to their documents can be achieved via the shared systems of Offce365 and Google.

2. The student will be reminded of the terms and conditions of our 'Pupil ICT Acceptable Agreement' and this will be fully emphasised and agreed, completed by a signature of evidence that this process has been fulfilled.

You'll be aware that we cannot jeopardise our own IT system in any way. If there is any breakdown in our network system and the issues are tracked back to the student's own laptop, we would have to look to you as parents to financially support this to be rectified. We are aware that the likelihood of this is extremely low however it does need highlighting from the out-set.

Agreement

Students and their parents/guardians wishing to take advantage of this opportunity, must comply with all rules and regulations set forth in this Agreement.

By choosing to participate you are consenting to the monitoring and verification of use, and to examination of the student's laptop as set forth above.

All violations of the above procedures may result in the confiscation, loss of privileges, the

student's parents contacted, and any consequences outlined in the Academy's code of conduct.

We have reviewed and agreed to these rules and regulations with my child.

Student Name _____

Student Signature _____

Parent/Guardian Name_____

Parent/Guardian Signature_____

Date_____

Agreement for Use of Student allocated Academy Laptop at Home

Alcester Academy defines a laptop computer as a portable microcomputer including electronic tablets and notepads. The purpose of these guidelines is to ensure that students recognize the limitations that the Academy imposes on the use of laptops for the purpose of safety and classroom integrity. In addition to these guidelines, the use of any computer in the Academy, including laptop computers, requires students to abide by the Academy's Pupil Acceptable Use Agreement which is available on the Academy's website.

There are many benefits for a student to regularly use a laptop. There are also many areas of caution which need to be considered.

General Usage

Alcester Academy is providing the opportunity for a student to use a laptop as an educational tool to increase learning and achievement. Student use of a personalised laptop will support educational instructional activities. The use of these laptops will be at the classroom teacher's discretion.

The student will:

1. use a personalised laptop to support the instructional activities occurring in the classroom.
2. obtain teacher permission before using a laptop regularly in class.
3. use only their assigned and authorized laptop.
4. not "lend" their laptop to another student during a lesson without clear instruction and full co-operation of the teacher.
5. turn off and put away a laptop when requested by a teacher.
6. not use their laptop in areas of the Academy that are outside of the classroom.
7. have their laptop confiscated, subject to teacher discretion, if found in violation of this agreement.

Security

Alcester Academy recognises that the loss or damage of possessions can be a very upsetting and traumatic experience and we need to clearly set out the position of all concerned to hopefully minimise the impact of such an event and to clearly lay out the Academy's position, should this occur.

1. Security of the laptop/tablet is the joint responsibility of the student and the Academy, and the student needs to carefully look after the equipment and consider using an Alcester Academy lockable locker if they wish to leave the laptop while they move elsewhere.
2. Academy owned allocated laptops that are stolen or damaged are the responsibility of the student and their parents or guardians.
3. Leaving equipment with someone else in the Academy can be very tempting but not recommended. You are responsible for any loss or damage and Alcester Academy will not support any claims against a third party in such circumstances.
4. A protective purpose designed laptop bag is provided for extra protection. It is possible to purchase back packs with purpose designed laptop carriers which are less detectable.

You may be able to find insurance through your home insurance policy or as a separate insurance agreement for this use.

Fit for Purpose

The IT Technical Support team will review the configuration and setup of the Academy Laptop to be issued, to make sure it is already fit for purpose, not damaged and fully tested for safe use.

If private software deemed appropriate for use by the student has been agreed, this will have to be configured by Alcester Academy IT Support team and so will require full instructions, copies of the software with licenses to enable them to install the software on the laptop.

The laptop will be configured so that both home and school Wi-Fi can be configured. When in school the usual filter system will be in place.

Network Security and Vulnerability

1. The Academy laptop **will** be configured to give full student access; the same as if using a workstation in school.

3. The student will be reminded of the terms and conditions of our 'Pupil ICT Acceptable Use Agreement' and this will be fully emphasised and agreed, completed by a signature of evidence that this process has been fulfilled.

You'll be aware that we cannot jeopardise our own IT system in any way. If there is any breakdown in our network system and the issues are tracked back to the student's laptop when used off site, we would have to look to you as parents to financially support this to be rectified. We are aware that the likelihood of this is extremely low however it does need highlighting from the out-set.

Students and their parents/guardians wishing to take advantage of this programme must comply with all rules and regulations set forth in this Policy.

Agreement

By choosing to participate you are consenting to the monitoring and verification of use, and to examination of the student's laptop as set forth above.

All violations of the above procedures may result in the confiscation, loss of privileges, the

student's parents contacted, and any consequences outlined in the Academy's code of conduct.

We have reviewed these rules and regulations with my child.

Print Student Name _____

Student Signature _____

Print Parent/Guardian Name_____

Parent/Guardian Signature_____

Date_____

Signed: _____Chair of Sub

Signed: _____Headteacher

Date: _____

(ratified by the Full Governing Body on 18th March 2025)