ICT and Telephone/Internet Acceptable Use Policy

Alcester Grammar School

Approved by:	Governing Board
Last reviewed on:	September 2025
Next review due by:	July 2026

CONTENTS

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 the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could 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, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur 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

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

Breaches of this policy may be dealt with under the relevant student behaviour policy/staff discipline policy & code of conduct.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- 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
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2024

- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **ICT facilities:** 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 that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's 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 agreed by an authorised user
- **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 school's 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 cybersecurity terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary (staff) or behaviour (student) sanctions (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
- 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 programme, tool or item of software designed to interfere with the functioning of the school's 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 the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel 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 or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Students using AI tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Principal or a delegated SLT member will use their 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 Principal's discretion.

Teachers may also decide to support students in using AI tools and generative chatbots for educational reasons:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example, in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

4.2 Sanctions

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

The student behaviour policy can be found on the school website. The Staff handbook is available to all staff via IamCompliant

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

5.1 Access to school ICT facilities and materials

The school's IT provider (EE) manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for specific programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT provider (EE).

Some staff will be issued with a personal or pool school laptop. This laptop is issued for work purposes, and colleagues are expected to treat the device with the same attentive care as they would a personal device. Staff must ensure that any laptop is connected to the school network, fully powered down, and then powered up again at least once a week during term time. Staff are expected to ensure that laptops are stored securely (a case is provided) and that screens are locked when not in use.

5.1.1 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. Staff should enable multi-factor authentication on their email account(s).

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/carers and pupils, and must not send any work-related materials using their personal email account. Staff should not engage in prolonged email conversations with students and/or parents outside of work hours. Staff should not communicate in regard to school matters with parents via home or personal mobile phone (text or talk), or messaging apps, nor communicate in regard to school matters with parents or students via social media such as Facebook, WhatsApp or a personal Twitter 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. Where possible 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 Principal and Finance and Operations Director immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

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.

It is against school policy to record a phone conversation. Staff who would like to record a phone conversation should speak to the Principal. All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Principal may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during pupil contact time
- 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 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 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with other elements of this policy.

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 pupils and parents/carers could see them.

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

5.2.1 Social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Staff must be aware that their role comes with particular responsibilities and they must adhere to the School's strict approach to social media.

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

- No student of the school, including sixth formers, should be a 'friend' of any member of staff. Privacy settings must be set up so that the profile for any member of staff is private, and only invited friends can access personal information.
- Staff are discouraged from social media and personal email contact with former students of the school, as there may be circumstances (such as late application to university) in which the member of staff may be considered to still be in a position of trust. In any event, it is recommended that, due to the potential risks, no member of staff should use their personal email or their social media accounts to be in contact with a former student unless the student is over 18 AND their school leaving date is more than 2 years ago. Any decision to communicate beyond this is taken at personal risk.

- Staff must not discuss students or colleagues or criticise the School or staff, online or on social media. Staff must also not post images that include students.
- Any concerns about the use of social media involving students should be discussed in confidence with the Principal, Vice Principal, or DSL as appropriate.
- Staff must not use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations. Staff must also not post disparaging or defamatory statements about our organisation, including other members of staff or governors, our students, suppliers and vendors, and other affiliates. Staff must also not use the internet or social media to harass or bully other members of staff.
- Staff should avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.
- Staff should report to their Head of Department or Line Manager immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School.
- Staff should make it clear in social media postings that they are speaking on their own behalf. Write in the first person and use a personal email address when communicating via social media.
- Staff are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by the masses (including the organisation itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.
- If you disclose your affiliation as an employee of the School, you must also state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present to students, parents and colleagues.
- Avoid posting comments about sensitive work-related topics, such as our performance. Even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.
- If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with the Principal. .
- Staff should immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other School policy.
- Do not post or publish anything on the internet or on any social networking site that your colleagues or our parents or students, governors, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.
- Do not post anything related to your colleagues or our students, parents, governors, business partners, suppliers, vendors or other stakeholders without their written permission.
- Staff should never provide references for other individuals on social or professional networking sites, as such references, whether positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

5.3 Remote access

School-owned Devices

All school-owned Laptops connect using an AOVPN (Always On VPN)
Only devices in an Active Directory security group are permitted to connect in this manner.
When in school, the device detects our network and connects just like any other computer in school.

When it doesn't detect the school network, i.e. on an external wifi connection, the AOVPN connects to our firewall, which allows the user to use the Laptop as if it were in school with access to school resources. Doing it this way also allows us to filter and monitor the internet connection as if it were an internal school device.

Non-school-owned devices (home computers or laptops)

Due to potential security concerns, access to systems from non-school-owned devices is being phased out as soon as possible. All staff who need access to school systems away from the school will be issued with (or be able to borrow temporarily from a pool) a school-owned device.

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.

Our school's data protection policy can be found on the school website.

5.4 Use of personal devices

This section applies to staff who use a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) for work purposes. It applies to use of the device both during and outside School hours and whether or not use of the device takes place at School.

This section applies to all devices used to access our IT resources and communications systems (collectively referred to as systems in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, PDAs, tablets, and laptop or notebook computers.

When you access our systems, you may be able to access data about the School, including information which is confidential, proprietary or private (collectively referred to as school data in this policy).

When you access our systems using a device, we are exposed to a number of risks, including from the loss or theft of the device, the threat of malware and the loss or unauthorised

alteration of school data. Such risks could result in damage to our systems, our business and our reputation.

Breach of this policy may result in our revocation of your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal.

5.4.1 Connecting devices to our systems

Connectivity of all devices to the School's systems is centrally managed by the school's IT Provider (EE), who must approve a device before it can be connected to our systems. We reserve the right to refuse or remove permission for your device to connect with our systems.

You are not permitted to connect any device to our system, other than a device that we have approved.

In order to access our systems, it may be necessary for the IT Provider to install software applications on your device. If you remove any such software, your access to our systems will be disabled.

For the avoidance of doubt, this does not include connecting personal devices to our WiFi network.

5.4.2 Monitoring

The contents of our systems and school data are our property. All materials, data, communications and information, including but not limited to email (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of business or on our behalf is our property, regardless of who owns the device.

We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device, whether or not the device is in your possession.

It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. You should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential.

Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law in order for us to comply with a legal obligation or for our legitimate school purposes, including, without limitation, in order to:

- prevent misuse of the device and protect school data;
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);
- monitor performance at work; and
- ensure that staff members do not use our facilities or systems for any unlawful purposes or activities that may damage the School, its systems or reputation.

We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

You acknowledge that the School is entitled to conduct such monitoring where it has a legal obligation or legitimate basis to do so, and that (without further notice or permission) we have the right to copy, erase or remotely wipe the entire device (including any personal data stored on the device).

Whenever we monitor personal data it will be carried out in line with the School's Telephone, Internet and Email Policy and government guidance such as KCSIE. This is also set out in the School's Staff Privacy Notice.

You acknowledge that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

5.4.3 Security requirements

You must comply with this policy when using your device to connect to our systems.

We reserve the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the school data on it for legitimate business purposes.

You must cooperate with us to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the device or relevant applications.

If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we shall immediately remove access to our systems and, where appropriate, remove any school data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or emails), it may not be possible to distinguish all such information from school data in all circumstances. You should regularly backup any personal data contained on the device.

You acknowledge that, without further notice or permission, we may need to inspect a device and applications used on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the data on or from a device for legitimate business purposes.

5.4.4. Lost or stolen devices and unauthorised access

In the event of a lost or stolen device, or where a staff member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to the school's IT provider (EE) r immediately.

Appropriate steps will be taken to ensure that school data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all school data on the device (including information contained in a work email account, even if such emails are personal in nature).

Although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or emails), it may not be possible to distinguish all such information from school data in all circumstances. You should regularly back up all personal data stored on the device.

5.5.5. Procedure on termination of employment

On your last day of work, or your last day before commencing a period of garden leave, all school data (including work emails), and any software applications provided by us for work purposes, will be removed from the device. If this cannot be achieved remotely, the device must be submitted to the school's IT Provider (EE) for wiping and software removal. You must provide all necessary cooperation and assistance in relation to this process.

5.5.6 Personal use

We have a legitimate basis or a legal obligation to access and protect school data stored or processed on staff devices, including the content of any communications sent or received from these devices. Where we are relying on our legitimate interests, we recognise the need to balance our need to process data for legitimate purposes with staff expectations of privacy in respect of their personal data.

Therefore, when taking (or considering taking) action to access personal devices or delete data on a personal device (remotely or otherwise) in accordance with this policy, we will, where practicable:

- consider whether the action is proportionate in light of the potential damage to the School, its pupils or other people impacted by school data;
- consider if there is an alternative method of dealing with the potential risks to the School's interests (recognising that such decisions often require urgent action);
- take reasonable steps to minimise loss of your personal data on the device, although we shall not be responsible for any such loss that may occur; and
- delete any such personal data that has been copied as soon as it comes to our attention (provided it is not personal data, which is also school data, including all personal emails sent or received using our email system).

To reduce the likelihood of the School inadvertently accessing staff personal data, or the personal data of third parties, staff must comply with the following steps to separate school data from their personal data on the device:

- organise files within the device specifically into designated folders that clearly distinguish between school data and personal data (for example, marking their own folders as "PERSONAL");
- do not use work email for personal purposes, but if this is necessary, ensure that it is labelled appropriately in the subject line; and
- regularly back up all personal data stored on the device.

5.5.7 Appropriate use

Staff must not use a device, including talking, texting, emailing, or otherwise, while operating a school vehicle or while operating a personal vehicle for school purposes. Staff must comply with any applicable law concerning the use of devices in vehicles.

5.5 School social media accounts

The school maintains several official Social Media accounts. No new accounts should be opened without the permission of the Principal. Staff members who have not been authorised to manage or post to the accounts, must not access, or attempt to access, the accounts.

5.6 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

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

The school monitors ICT use to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards

- 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

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns.
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) supported by the DDSL and Vice Principal will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL , as appropriate.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suites and classrooms are available to pupils only under the supervision of staff
- Sixth-form pupils can use the computers in study rooms independently, for educational purposes only

6.2 Search and deletion

Under the Education Act 2011, the Principal, and any member of staff authorised to do so by the Principal, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out (your behaviour policy should list these items), **and/or**

- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Principal
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the school's behaviour policy,
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the Principal or Vice Principal to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils and staff, in line with the behaviour or discipline 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 making 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 or 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 the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

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

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

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

7.2 Communicating with or about the school online

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

Parents/carers 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/carers to sign the agreement in appendix 2.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls

- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 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.

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

8.2 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 have these installed, and 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.

8.3 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 website.

8.4 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 school's IT provider (EE)

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 school's IT provider and the Principal 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 shut down completely at the end of each working day.

8.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption. USB drives do not work on the school site.

9. Protection from cyber attacks

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

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure

Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school'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 school will verify this using a third-party audit (Cyber Essentials at least annually, to objectively test that what it has in place is effective
  - **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 school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data at least daily
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT Provider (EE)

- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan 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 school's wireless internet connection is secure.

- All wifi connections are filtered in the same way as the computers in school
- Our Wifi is separated into VLANs.
- Only Staff and students in years 12 and 13 have access to the WIFI
- Guests have access to the Wifi by using a portal and a ticketing system on AGS-Guest, they receive a code from reception and use VLAN 14

We receive daily reports of all sites visited using Sophos Reporter whether they are filtered or not.

10.1 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

The Principal will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTFA)
- 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)

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

11. Monitoring and review

The Principal and IT Provider (EE) 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 2 years.

The governing board is additionally responsible for approving this policy.

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 main channels : • Our website • Email/text groups for parents via GroupCall (for school announcements and information) • Satchel One • Evolve • BlueSky We are also aware that parents/carers 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). **The school does not formally support such groups and warns parents and carers of associated dangers with informal second-hand communication - however, we recognise that these can be of some benefit to some parents and carers on occasion.**
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 social mediator personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way

• Use private groups, the school's social media or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. 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 names or photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**

Appendix 2: Acceptable use agreement for pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
I agree to abide by all elements of this Acceptable ICT and Internet Use Policy **In particular when using the school's ICT facilities and accessing the internet in school, I will not:** • Use them to break school rules • Access any inappropriate websites • Open any attachments in emails without first considering if…cyber safe • Use any inappropriate language when communicating online, including in emails • Share any semi-nude or nude images (whether real or generated), videos or live streams, even if I have the consent of the person or people in the photo/video • Share my password with others or log in to the school's network using someone else's details • Bully other people • Use AI tools and generative chatbots (such as ChatGPT or Google Bard): o During assessments, including internal and external assessments, and coursework o To present AI-generated text or imagery as my own work 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 (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet. I agree to the conditions set out above for pupils 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:**

Alcester Grammar School

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:	
I agree to abide by all elements of this Acceptable ICT and Internet Use Policy 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 • 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 any private business, 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 IT Provider (EE) 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 school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Glossary of cybersecurity 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.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
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.

TERM	DEFINITION
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.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as 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.

TERM	DEFINITION
Virus	Programmes 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 people in an organisation.