AVANTI SCHOOLS TRUST

Acceptable Use Policy

Summer 2024

Review date: Summer 2025

ACCEPTABLE USE POLICY

This policy is in force until further notice from:	Summer 2024
This policy must be reviewed by no later than*: **this refers to the term in which the Policy must be reviewed by the appropriate Committee for recommendation to the Board.*	Summer 2025
Policy Author(s):	Head of Digital & IT
Date policy reviewed by Committee and Minute reference	Audit & Risk Committee: 04.07.24 (Minute reference 6)
Date Policy approved by the Trust Board and Minute reference	23.07.24 (Minute reference 118)
Location of publication of policy:	Governor Hub/ AST Website/ Internal Records and Intranet

1. Introduction and Aims

ICT is an integral part of the way our schools work, and is a critical resource for pupils, staff, SSC members, Trustees, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the schools.

The ICT resources and facilities our schools use 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, SSC members and Trustees across the whole of Avanti Schools Trust.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policy on data protection, online safety and safeguarding.
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems.
- Support the school in teaching pupils safe and effective internet and ICT use.

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

Breaches of this policy may be dealt with under our Disciplinary Policy.

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 2020
- Searching, screening and confiscation: advice for schools

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 IT Team to use the ICT facilities, including Trustees, SSC members, staff, pupils, volunteers, contractors, visitors, and other AST subsidiaries.
- **"Personal use":** any use or activity not directly related to the users' employment, study, or job purpose.
- **"Authorised personnel":** employees and contractors authorised by the school to perform systems administration and/or monitoring of the ICT facilities.
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

4. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary proceedings (see section 4.3 below).

Unacceptable use of the school's ICT onsite facilities (and at any other time offsite) includes:

- **Personal Use**: Using school ICT for personal activities such as banking, shopping and personal email.
- **Intellectual Property**: Breaching intellectual property rights, such as copyright.
- **AI Platforms**: Using company or confidential data on AI platforms like ChatGPT, Copilot, Gemini, etc.
- **Bullying and Harassment**: Using ICT to bully, harass, or promote unlawful discrimination.
- **Policy Breaches**: Violating any school policies or procedures.
- **Illegal Activity**: Engaging in illegal conduct or promoting illegal activities.
- **Inappropriate Material**: Accessing, creating, storing, or sharing pornographic, offensive, obscene, or inappropriate content.
- **Defamation**: Defaming or disparaging the Trust/school(s) or risking its reputation.
- **Confidential Information**: Sharing confidential information about the school(s), pupils, or staff with unauthorised individuals.
- **Unauthorised Devices**: Connecting devices to the school's network without approval.
- **Software and Tools**: Installing software or web services on the school's network without approval or using tools that interfere with ICT operations.
- **Unauthorised Access**: Gaining or attempting to gain access to restricted areas or password-protected information without authorisation.
- **Encouraging Unauthorised Access**: Allowing others to gain unauthorised access to ICT facilities.
- **Intentional Damage**: Causing intentional damage to ICT facilities.
- **Unauthorised Removal**: Removing, deleting, or disposing of ICT equipment or information without permission.
- **Data Breaches**: Accessing, modifying, or sharing data without authorisation.
- **Offensive Language**: Using inappropriate or offensive language.

- **Private Business**: Promoting private businesses without approval.
- **Bypassing Filters**: Using websites or VPNs to bypass the school's filtering mechanisms.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Principal or any other senior member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1. Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Principal or Exec member and area IT manager's discretion. Please submit a request to the Principal and IT Manager for approval via email.

4.2. Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's Disciplinary Policy.

If required, the Principal or Exec member can request access to be revoked immediately from any member of staff or student until an incident has been resolved.

5. Staff (including SSC Members, volunteers and contractors)

5.1. Access to school ICT facilities and materials

The school's IT manager/Engineer manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices.
- Access permissions for certain programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school'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 the IT manager/Engineer by raising a ticket using the web form, with information about what access is required and including any approvals for the owner of that information, i.e. Finance Lead, Head of Department.

5.2. One Computer Device Policy

To ensure equity and consistency, all staff are limited to one computer device, which will be either a laptop, tablet or desktop, depending on their role requirements. Additional devices will only be provided if staff can prove and justify that they cannot perform their job properly with only one device. Such exceptions must be expressly sanctioned by the Head of IT. This policy helps to maintain fairness and effective resource allocation across the Trust.

5.3. Use of ICT Facilities for Communications

- **Email Usage**: Use your school-provided email address for all work-related communications. Do not use personal email accounts for work purposes or share your personal email address with parents or pupils.
- **Email Content**: Be cautious with email content to avoid issues like discrimination, harassment, defamation, breach of confidentiality, or breach of contract. Remember, email messages may need to be disclosed in legal proceedings.
- **Handling Sensitive Information**: Use secure methods, such as encryption or OneDrive secure links, when sending sensitive or confidential information via email. Treat all emails as potentially retrievable.
- **Email Errors**: If you receive an email by mistake, inform the sender and delete it. Do not use or disclose the information. If you send an email containing personal information by mistake, inform the IT manager/Engineer immediately and follow the Data Breach Procedure.
- **Phone Numbers**: Do not give your personal phone number to parents or pupils. Use school phones solely for work purposes.
- **Mobile Phones**: Follow the same ICT Acceptable Use rules for school-provided mobiles.
- **Call Recording**: All calls to and from the school office are recorded for administrative support and staff training purposes.

5.4. Personal Devices to Access Avanti ICT Facilities

- **Impact of Personal ICT Use:** Personal use of ICT can affect employment by exposing personal details to pupils and parents.
- **Information Disclosure:** Information generated in school may be disclosed under the Freedom of Information Act 2000 and made public.
- **Follow Guidelines:** Adhere to the school's social media (see appendix) and use of email guidelines (see section 5.3) to protect yourself online and maintain professional integrity.

5.5. Personal Social Media Accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.6. School Social Media Accounts

The school has an official Facebook/X/Instagram page, managed by Avanti's marketing team. Staff members who have not been authorised to manage, or post to, these accounts, must not access, or attempt to access these accounts.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the accounts must ensure they abide by this policy at all times.

5.7. Monitoring of school network and use if ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.
- Any other electronic communications, including AI services.

Only authorised ICT staff or authorised teaching staff may inspect, monitor, intercept, assess, record and disclose the above. This will only ever be to the extent permitted by law and as necessary and justifiable for work-related purposes.

The school may monitor 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.

The following information will be provided to employees subject to monitoring:

- **Circumstances**: Monitoring may take place when an employee is on long-term sickness or absence, or when there is a suspicion of inappropriate use or security breaches.
- **Nature of Monitoring**: Monitoring may include reading, reviewing or archiving emails.
- **How Information is Used**: Information obtained through monitoring will be used to maintain school operations, ensuring compliance with policies and regulations, and investigate any concerns or breaches.
- **Safeguards**: The school has implemented appropriate safeguards to protect the privacy and confidentiality of employees subject to monitoring, including limiting access to information to authorized personnel only and ensuring data security measures are in place.

Additionally, we want to make sure that you have a clear understanding of the following:

- **When Information is Obtained**: Information may be obtained during the monitoring period, which will be limited to the time period necessary to achieve the purpose of monitoring.
- **Why Information is Obtained**: Information is obtained to ensure that the school can continue to operate effectively and securely, and to comply with policies and regulations.
- **How Information is Used**: Information obtained will be used solely for the purposes of monitoring and maintaining school operations, and will not be used for any other purposes.
- **Disclosure of Information**: Information obtained will be disclosed only to authorised personnel who have a legitimate need to know, and only to the extent necessary to achieve the purpose of monitoring.

6. Pupils

6.1. Access to ICT facilities

ICT facilities should only be made available to pupils under the following circumstances:

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff.
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff.
- Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device.
- Pupils can use the computers in a location outlined by a Principal independently for educational purposes only.

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 school has the right to search pupils' personal phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

7. Parents

7.1. Access to ICT facilities and materials

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

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

The school believes 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 school through its website and social media channels such as Facebook/Instagram/Twitter or any other group messaging or social platform.

Parents are requested to sign the agreement in the appendix, when onboarded to one of our schools.

8. Data Security

The school takes steps to protect the security of its computing resources, data, and user accounts. However, the school cannot guarantee security. Staff, pupils, parents, and others who use the school's ICT facilities should use safe computing practices at all times as detailed below.

8.1. Passwords

- All users must set strong passwords (8-10 characters, including one capital letter and a number) and keep them secure.
- Users are responsible for their passwords, account security, and setting permissions for their accounts and files.
- Disclosing account or password information may result in disciplinary action for staff and pupils, or revoked access for parents and volunteers, in line with the School Behaviour Policy:
    - Staff passwords are provided to their line manager only.
    - Pupil passwords are provided to the BSM or ICT Lead.
    - Passwords must not be written down; use a reputable password management system.
    - If an account is compromised, change the password immediately and notify line management/Teacher/IT Manager/Local IT Engineer.

8.2. Multi-factor authentication

To enhance the security of our IT systems and protect sensitive information, all staff are required to use Multi-Factor Authentication (MFA) when accessing school-related accounts and services. MFA provides an additional layer of security by requiring not only a password and username but also something that only the user has on them, i.e., a piece of information only they should know or have immediately to hand – such as a physical token, a mobile app or your company device.

Staff must set up MFA on their accounts as directed by the IT department. Instructions and support for enabling MFA will be provided during onboarding and are available on the school's intranet. This measure helps to ensure that even if a password is compromised, the account remains secure. Compliance with MFA is mandatory and will be monitored regularly. Any issues with MFA setup or usage should be reported to the IT department immediately.

8.3. 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 be configured to perform such updates regularly or automatically.

Where automatic updates are not available, staff are expected to maintain a 'ready to work' approach and apply updates as required.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards the school implements and maintains to protect personal data and the school's ICT facilities.

8.4. Data protection

All personal data must be processed and stored in line with relevant law and the Trust's Data Protection Policy and other related policy and procedure.

8.5. Access to facilities and materials

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

- **Access Rights**: Managed by line manager/ICT lead/teacher/engineer.
- **Unauthorized Access**: Users must not access systems, files, or devices without permission. Report accidental access immediately.
- **Logging Out**: Always log out and lock equipment when not in use. Fully log out and shut down at the end of each day.
- **ICT Equipment Issuance**: Logged and recorded in the Trust/School inventory via the AST IT Equipment Loan Form.
- **Visitor Restrictions**: Visitors must not connect their hardware to the school network (unless special provision has been made). Direct them to guest Wi-Fi if available.
- **Physical Security**: Keep ICT equipment secure when not in use. Lock away portable devices overnight.

- **Data Backup**: Regularly save data to the school's network. Staff are responsible for backing up and restoring their own data.
- **End of Employment**: Return all ICT equipment to the manager.
- **Information Security**: Keep information accessed from Avanti devices or removable media secure. Do not disclose personal, sensitive, confidential or classified information to unauthorized persons.
- **Wi-Fi Access**: Access for school leavers will be removed. Temporary guest access is restricted and authorised for limited periods by an Avanti staff member.

9. Internet access

The school's internet connection is secured.

- Schools have a filtered and monitored connection.
- Report any inappropriate sites that the filter hasn't identified to the safeguarding lead.

9.1. Pupils

Instances in which the school may provide Wi-Fi for student device use:

- Wi-Fi will be segmented and visible with a specific name, such as BYOD.
- Access to the connection will be reliant on a username and password. All connections are monitored and filtered.
- Pupils can request access if the network is available by asking their teacher/admin staff.

9.2. Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless they are sponsored access by a member of staff, such as:

- Parents are working with the school in an official capacity (e.g. as a volunteer).
- Visitors and Lettings who need to access the school's Wi-Fi 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 Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

9.3. Monitoring and review

The Principal and Head of IT monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school. This policy will be reviewed every 2 years. The governing board Audit and Risk is responsible for approving this policy.

10. Related Policies

This policy should be read alongside the following Trust policies which can be found on the website and/or the pupil/staff intranet:

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Disciplinary Policy
- Online Safety and Remote Learning Policy
- Behaviour Principles Written Statement

11. Appendix 1: Social Media Guidelines for Staff

Given the diverse range of social media platforms available today, it is important for staff to follow guidelines that ensure professionalism and protect the reputation of the school. This appendix provides guidelines for the use of popular social media and messaging platforms.

11.1. General Guidelines

- **Professionalism**: Maintain professionalism in all online interactions. Avoid posting content that could be seen as offensive or inappropriate.
- **Privacy Settings**: Regularly review and adjust privacy settings to control who can see your posts and personal information.
- **School Representation**: Do not represent yourself as speaking on behalf of the school unless explicitly authorised to do so.
- **Friend Requests**: Do not accept friend requests from students or parents to maintain professional boundaries.
- **Content Sharing**: Be cautious about sharing personal opinions or content that could be misconstrued. Ensure that any shared content is appropriate and reflects well on the school community.

11.2. Platform-Specific Guidelines

- **Facebook**: Follow the existing guidelines in Appendix 1. Additionally, be mindful of tagging colleagues and avoid sharing posts that may reflect poorly on the school.
- **Twitter**: Use Twitter for professional networking and sharing educational content. Avoid engaging in arguments or sharing sensitive information.
- **Instagram**: Set your profile to private if using it for personal purposes. If using Instagram for professional reasons, ensure that all content is appropriate and educational.
- **LinkedIn**: Utilise LinkedIn for professional networking and sharing career-related updates. Maintain a professional tone and be mindful of your connections and interactions.
- **WhatsApp**: Use WhatsApp groups for professional communication only if they are school- sanctioned. Avoid sharing sensitive information in group chats.
- **TikTok**: If using TikTok, ensure that all videos are appropriate for a professional setting. Avoid participating in trends that could be seen as unprofessional.
- **Snapchat**: Given the ephemeral nature of Snapchat, it is recommended to avoid using this platform for any professional interactions or sharing of school-related content.

11.3. Responding to Online Issues

- **Harassment or Bullying**: If you experience harassment or bullying online,

document the incidents and report them to senior leadership. Do not engage with the perpetrator.

- **Negative Comments**: Do not respond to negative comments about the school. Instead, report them to the designated school representative for appropriate
  Handling.
- **Privacy Breaches**: If you accidentally share sensitive information, delete the post immediately and inform senior leadership.

11.4. Social Media for School Purposes

- **Official Accounts**: Only designated staff should post on the school's official social media accounts. Ensure that all posts are in line with the school's communication policy.
- **Content Approval**: All content intended for official school accounts should be reviewed and approved by the relevant authority before posting.

11.5. What do to if…

A pupil adds you on social media
• In the first instance, ignore/delete the request. Block the pupil from viewing your profile. • Check your privacy settings and consider changing your display name or profile picture. • If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages. • Notify the senior leadership team or the Principal about what's happening.
A parent adds you on social media
It is at your discretion whether to respond. Bear in mind that: • Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school. • Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in. If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.
You're being harassed on social media, or somebody is spreading something offensive about you
• **Do not** retaliate or respond in any way.

- Save evidence of any abuse by taking screenshots and recording the time and date it occurred.
- Report the material to the relevant social network and ask them to remove it.
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents.
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material.
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.