IT Acceptable Use Policy

1. Introduction

This policy is used to define the acceptable use of IT systems by all members of the school community (users).

The policy applies to all users of IT systems with appendices providing additional policies for specific cohorts of users. These are:

- Pupils of secondary and sixth form education;
- Students of higher education;
- Staff, including freelance staff and members of the Board of Trustees.

IT systems are defined as:

- Computers or mobile devices owned or managed by the school;
- Computing resources provided to any device using the school's on-premises or cloud infrastructure;
- Access to the internet on-campus using any device;
- Cloud services provided by the school such as email, online storage, and video meeting services;
- Any future IT service the school decides to provision to support learning or business operations;
- Data held in databases, or any other storage managed by the school.

This policy aims to:

- Promote the professional, ethical, lawful, and productive use of IT systems;
- Define and identify unacceptable use of any IT systems, provided by the school or externally;
- Remind users about the importance of security and data protection;
- Describe why monitoring takes place on the use of the school's IT systems;
- Describe and identify unacceptable use of social media;
- Specify the consequences of non-compliance.

If you are in doubt and require clarification on any part of this document, please speak to the Head of IT.

2. Provision of IT Systems

2.1. All equipment, software, service, or intellectual property that constitutes the schools IT systems is the sole property of the school.

2.2. Users must not try to install any software on school IT systems without permission from the Head of IT. Users may be held personally liable for costs incurred due to damage to the schools IT systems caused by the unauthorised installation of software.
2.3. The Head of IT is responsible for purchasing and allocating equipment to individuals. Equipment may be removed at any time, without warning, for regular maintenance, reallocation, or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.
2.4. Users are not permitted to make any physical alteration, either internally or externally, to school equipment.

3. Authentication and Security

3.1. All users must be registered, and credentials created before accessing any IT system. New accounts and modification to accounts can only be requested by specific staff members (see appendices).
3.2. Following account creation credentials are provided, consisting of a username, password, and an email address. All passwords should be complex to ensure data and network security (see also 3.11 below). All user account details are for the exclusive use of the individual to whom they are allocated. Users are responsible for ensuring their password remains confidential and their account is secure.
3.3. Users are expected to enrol in account recovery services. This takes place at account creation and users are requested to enrol additionally with Microsoft Azure AD self-service at https://aka.ms/ssprsetup.
3.4. All users are personally responsible and accountable for all activities carried out under their user account. Users must take all reasonable precautions to protect their user account details and must not share them with any other person except to members of the IT department for the purposes of support.
3.5. Users must report any security breach for any user account, or IT service, to the IT department as soon as possible.
3.6. Users should only access IT systems and data for which they are authorised to access.
3.7. Unattended devices must either be logged off or locked by the last user.
3.8. The school installs antivirus, antimalware, and other security software on all devices. Users are not permitted to attempt to install additional security software on school devices.
3.9. Users must not attempt to tamper with, or bypass, any security software, authentication system or other security system implemented by the school.
3.10. Internet activity must not compromise the security of the data on the school IT systems or cause disruption for any other users.
3.11. Users are expected to exercise best practise to ensure their school account remains secure. This includes:
    3.11.1. Reporting of a suspected breach to the IT department as soon as possible.
    3.11.2. The use of a complex password including uppercase and lowercase characters, numbers, and symbols.
    3.11.3. The use of a unique password for a school account, not used by the user on any other service.
    3.11.4. Immediately resetting or changing the account password as soon as a breach is suspected.
3.12. The school reserves the right to revoke access to any IT services for security reasons or if instructed by senior staff.

4. Electronic Communications

4.1. Your school digital identity includes your email account, access to instant messaging and video conferencing platforms and user profiles related to IT systems provided by the school.
4.2. All school-related communications must take place using identities provided by the school. Communication between staff and students or staff and pupils using personal email, social media, instant messaging, or any other non-school service is strictly forbidden.
4.3. Professional etiquette is expected by all users when communicating.

4.4. Language used in communications must not be offensive or abusive.
4.5. Content of a pornographic, illegal, violent, sexist, extremism or terrorism related, or discriminatory nature is strictly forbidden.
4.6. The school monitors electronic communications for offensive, abusive, pornographic, violent, sexist, discriminatory and illegal content.
4.7. The school monitors electronic communications for content that may indicate a safeguarding concern.
4.8. The school monitors electronic communications for content that may indicate a risk of extremism.
4.9. The downloading, storing, or sharing of content which contains copyright material (e.g., films, music, eBooks and other publications) for which the users or school does not have distribution rights is not permitted.
4.10. The forwarding or distribution of spam and junk messages is not permitted.
4.11. Access to digital communication systems will always take place in accordance with data protection legislation and in line with other appropriate school policies.
4.12. Members of the community must immediately report to relevant staff if they receive offensive communication, and this will be recorded in relevant records.
4.13. School email addresses and other official contact details must not be used for setting up personal social media accounts or any online services unrelated to the school's business.
4.14. Communications should avoid personal opinions about other individuals.
4.15. Any user who encounters prohibited content described in section 4 on a School IT system should report this immediately to the Head of IT, Principal, or other relevant member of staff such as the Designated Safeguarding Lead.

5. Internet Access

5.1. Internet access is provided primarily for educational and professional use, with reasonable personal use being permitted.
5.2. Content is filtered by enterprise connection filtering. Inappropriate material is generally blocked. On occasion it may be possible to access inappropriate material, where this has been misclassified by the filter. Such content should be reported immediately to the IT department.
5.3. User connections to the school network are authenticated and internet usage is monitored and recorded. Users are liable for all activity carried out under their credentials.
5.4. Users must not attempt to access any material which could be regarded as illegal, offensive, in bad taste or immoral.
5.5. Misuse of the internet may, in certain circumstances constitute a criminal offence and accessing or sharing any of the following content will result in disciplinary action:
    5.5.1. Pornographic content of any kind, including video, image or written.
    5.5.2. Racist or discriminatory content.
    5.5.3. False or defamatory comments or content about another individual or organisation.
    5.5.4. Content which incites hate or content of an extremist nature which indicates a risk of terrorism, however minor.
    5.5.5. Any statement or content which is likely to cause any liability, whether criminal or civil, and whether to an individual or the school.
    5.5.6. Content which discloses to unauthorised recipients, confidential information about the school, members of the school community or third parties.
    5.5.7. Any content which presents a risk of harm to a child.
5.6. Online gambling is not permitted.
5.7. The school reserves the right to employ traffic shaping and to prioritise bandwidth for educational and professional purposes, for instance, to restrict the use of services (e.g., streaming) on certain networks or to set a bandwidth speed limit for groups of users to ensure essential business operations are not impacted.

5.8. Whilst every effort is made to ensure internet access is available, the school is not liable for any damages, loss of data, or academic penalty caused by a loss of connectivity.
5.9. The school is not liable for damage to any personal device caused by downloading any content from its internet connection.

6. Social Media

6.1. All members of the school community have a responsibility to protect the reputation of the school and are expected to act with respect when using social media.
6.2. Social media exchanges between staff and students, or staff and pupils are not permitted. This includes soliciting or accepting a friend request, commenting on personal posts, or joining private groups on social media.

7. Support

7.1. All users are asked to use the email address helpdesk@artsed.co.uk to request support.
7.2. If urgent, users may request support by calling 020 8987 6656.
7.3. Users must not attend the IT office without prior appointment.
7.4. When requesting support users must provide full details of the issue or request and give a contact telephone number. IT are unable to deal with requests without sufficient information.
7.5. The use of a personal telephone number is permitted as an exclusion to the restrictions outlined in this policy. IT do not maintain records of this contact information and will only use this to facilitate support.
7.6. In order for IT to address requests effectively, users must not raise multiple issues in a single request, i.e., a to do list. IT will be unable to deal with such multiple requests.
7.7. Although best endeavours are made to respond quickly to support requests, the IT department must prioritise requests to meet the needs of the organisation and with the available support resources. The IT department cannot guarantee an immediate response to any request
7.8. Users will be courteous and professional when interacting with support staff. Behaviour or communications that could be considered obstructive, abusive, or offensive are not acceptable and will be reported to the Head of IT.

8. Monitoring of IT Systems

8.1. The school exercises its right to monitor the use of IT systems. This includes web content and application (i.e., mobile device apps) usage, the interception of digital communications and the viewing of content or data stored by a user.
8.2. Any inappropriate content discovered will be either deleted or reported to the appropriate internal authority. Where deemed necessary, it will be reported to the relevant external authority such as the police, a safeguarding authority or counterterrorism.
8.3. Monitoring of IT systems takes place by the Head of IT for the following reasons:
    8.3.1. To ensure operational effectiveness of IT systems.
    8.3.2. To identify safeguarding or behavioural concerns.
    8.3.3. To prevent a breach of the law, this policy, or any other school policy.
    8.3.4. To investigate a suspected breach of the law, this policy, or any other school policy

9. Failure to Comply with the Policy

9.1. Where it is found that a breach of this policy has taken place a disciplinary procedure may be invoked which can result in exclusion or dismissal.

9.2. If a user suspects there has been a breach of this policy this should be reported to the Head of IT, or another senior member of staff as soon as possible.
9.3. Any unauthorised use of the school's IT systems which may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police, safeguarding authority, counterterrorism, or other relevant authority.
9.4. The school reserves the right to audit, suspend or terminate any user account or IT service pending an enquiry, without notice to the user(s) concerned.

10. Appendix A: Pupils of Secondary and Sixth Form Education

10.1. This policy should be read in conjunction with the Online Safety Policy.
10.2. Pupils and their parents or guardians must read this policy, and the Online Safety Policy in full. Accessing any school IT service is considered as demonstrating agreement to this policy.
10.3. Pupils will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
10.4. If Pupils use their own devices in the school, they will follow the rules set out in this policy, in the same way as if they were using school equipment.
10.5. Pupils must only engage with staff digitally using services provided by the school and must never attempt to contact staff using personal email, instant messaging such as WhatsApp, Facebook Messenger, Snapchat, LinkedIn or similar, or any social media.

11. Appendix B: Students of Higher Education

11.1. Students must only engage with staff digitally using services provisioned by the school and must never attempt to contact staff using personal email, instant messaging such as WhatsApp, Facebook Messenger, Snapchat or similar or any social media.
11.2. The school will delete student accounts within five calendar months from withdrawal or graduation. The school account should not be used for communications with third parties if later access will be required; similarly, accounts should not be used for the storage of data that may be required by the student after leaving the school.
11.3. Students graduating from third year BA courses may, at the discretion of the Head of IT, be given an alumni email address. Students should read the IT Services for Graduating Students Policy for further information.

12. Appendix C: Staff

12.1. The use and monitoring by the school of electronic communications is likely to involve the processing of personal data; it is therefore regulated by the Data Protection Act 2018 and the 2020 update to include the UK General Data Protection Regulation, together with the Employment Practices Data Protection Code issued by the Information Commissioner. A data breach caused by the misuse of IT systems, including the loss of an inadequately secured device, may be reported to the Information Commissioner. Staff are referred to the Data Protection Policy for further information.
12.2. Staff user accounts are additionally secured using multi-factor authentication and staff are required to ensure registration in any additional security measures as deemed necessary.
12.3. Staff are required to use their personal mobile phone solely for the purpose of multi-factor authentication.
12.4. Under no circumstances should a member of staff allow a pupil or student to use their account for any purpose. This includes access to a device that is authenticated with a staff account.
12.5. Access to data and services is provided on an as needed basis with justification and appropriate authorisation.

12.6. Staff accounts do not have any access to shared folders by default. All access must be by request to the IT helpdesk.
12.7. If requesting an elevation of permissions, i.e., access to a shared folder, staff should copy in their line manager for approval. IT will disregard requests that are not accompanied by appropriate authorisation.
12.8. Any communication which contains any content which could be subject to data protection legislation such as sensitive or personal information (as described by the Data Protection Policy and including assessment outcomes) should only be sent using secure and encrypted methods.
12.9. Communications should never contain the full name of pupils or students either in the subject line or the main body of text. Initials or an alternative non-identifying reference should be used.
12.10. Staff are encouraged to develop an appropriate work and life balance and when sending communications. They should avoid sending communications between 19:00 and 07:00 on workdays, at weekends and during full closure periods.
12.11. Communications sent to external parties should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
12.12. All items in policy paragraph 5.5 constitute gross misconduct.
12.13. The use of online dating and similar platforms is not permitted at school.
12.14. Mobile devices are permitted at school, but their use should be kept to a minimum and they should not be used when directly supervising pupils or students.
12.15. Personal cameras, including those on mobile phones must not be used for photographs of pupils or students under any circumstances. The school will provide appropriate equipment if required and images should be stored securely in a restricted file share and immediately deleted from the device.
12.16. Personal phone numbers should not be shared with parents, pupils or students under any circumstances and all telephone communications must be made using school-owned devices.
12.17. Staff are provided with a personal quota of online storage and given access to organisational file shares as required. All work-related data should be stored in these locations.
12.18. Staff are responsible for ensuring that they, or the school, has rights to use any copyrighted material.
12.19. The use of external storage media is restricted and only allowed where a justifiable business requirement exists. This must be approved by the Head of IT.
12.20. To facilitate remote working the school may make some data available from a personal device through a web browser. It is not permitted to download or store any organisational data on a personal device.
12.21. It is permitted to access school data from a personal mobile device. This is only permitted with the enrolment of the device with the device compliance system, and accessing data is only possible through authorised applications such as Microsoft Outlook or Microsoft Teams. Data cannot be downloaded to a personal device.
12.22. The use of an individual's social media account for school business is not permitted, unless via a school recognised account or with the permission of the Head of Development and Marketing.
12.23. Members of staff will notify the Director of Development and Marketing if they consider that any content shared or posted via any information and communications technology, including emails or social media, conflicts with their role in the school setting.
12.24. No images or videos which show members of the school community should be shared on social media or other sites other than by the Development and Marketing department.
12.25. No confidential school data should be posted on social media, including communications, images, video, or documents.
12.26. No details or opinions about pupils or students should be posted on social media.
12.27. No opinions regarding another member of staff which could cause offence should be posted on social media.
12.28. The school may access a staff mailbox if necessary to maintain business continuity; this may include the delegation of a mailbox to another member of staff, the redirection of incoming email, or the retrieval of messages.

Title of Policy	IT Acceptable Use Policy
Maintained By	Head of IT
Owned By	Head of IT
Approving Committee / Ratifying Body	
Last Reviewed on	
Review on	1
Current Version	
Location of master document	
Web location	