School - Acceptable Use of IT Policy

Version Date	Date of next review
September 2023	

Purpose

Information technology is an integral part of the way we work, and is a critical resource for students, staff, parents, volunteers and visitors. It supports teaching and learning, including the pastoral and administrative functions of our schools.

This Acceptable Use Policy outlines how Artemis expects people to behave when they are online, and/or using school networks, connections, internet-based resources, personal electronic devices, cloud platforms and social media (both when on school site and outside of YOURNAME and work)[1]. Parents, students, staff, and visitors who do not acknowledge this policy in its latest version may be denied access to IT resources.

Policy: acceptable use

We expect all users of technology and online platforms to act in line with Artemis values, and to interact respectfully with people and the digital environments in which they work and learn:

1. Be polite, do not be abrasive in your communication to others
2. Use appropriate language
3. Note that the online space is not a place where privacy can be guaranteed
4. Privacy is difficult to assure in public-available platforms, and digital information is very difficult to remove/delete from devices and platforms
5. Respect the intellectual property of other users and information providers
6. Respect the privacy of others with regard to use of images, video and other content

Policy: unacceptable use

Unacceptable use of IT facilities includes:

- using IT facilities to breach intellectual property rights or copyright
- using IT facilities (including any Artemis IT account or service) to bully or harass someone else, or to promote unlawful discrimination (for example comments that breach a person's rights under the Equality Act 2010, and in particular the protected characteristics cited in that Act), or that could damage the reputation of Artemis and/or its schools
- breaching IT policies or procedures
- cyberflashing

[1] Where Artemis Education operates outside of the United Kingdom, the UK regulatory framework will provide the foundation for best practice as far as this policy is concerned. All Artemis schools will operate in compliance with the relevant legislation of the country in which they are operating. This policy has been created in accordance with guidance provided in The Education (Independent School Standards) Regulations 2014 Part 3, 7(a), 8(a) and 9(a) & (b), along with the provisions for Online Safety outlined in Keeping Children Safe in Education and associated guidance. In particular, Artemis as a data controller recognises and aims to abide by our responsibility to protect and uphold the rights of data subjects as outlined in Chapter III of the General Data Protection Regulations and Part 2 Chapter 2 of the Data Protection Act 2018.

- 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 harassing or offensive images and/or videos and/or livestreams
- activity which defames or disparages YOURNAME, or risks bringing the school into disrepute
- sharing confidential information about the school, its students, or other members of the school community
- connecting any device to the school's IT 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 IT 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 IT facilities
- causing intentional or reckless damage to the school's IT facilities
- removing, deleting or disposing of the school's IT 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 online
- assuming the digital identity of others, acting falsely, or taking digital actions that affect others without their permission
- promoting a private business, or undertaking unethical, disruptive, personally damaging, or unapproved commercial activity
- 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
- misusing, tampering with, altering, stealing, vandalising, defacing, or intentionally damaging any Artemis technology
- disseminating "SPAM" (unsolicited commercial and non-commercial e-mail) or initiating or participating in the promulgation of chain letters, unauthorised automated or mass postings, or other types of unauthorised large-scale distributions
- invading the privacy of, or inappropriately distributing the phone number(s), e-mail addresses, or other personal information of, another person
- posting confidential information on the Internet about Artemis, its schools, customers, suppliers, staff, students or volunteers

This is not an exhaustive list. The Artemis Director of Education, Head of School or Director of Education will use their professional judgement to determine whether any act or behaviour not listed above is considered unacceptable use of IT facilities. Any exception to this policy must be approved in writing by a member of the Artemis Education Office.

Policy sanctions
All users must agree to comply with this policy as well as with other applicable laws, rules, policies and regulations. Access to technology is a privilege which the organisation can suspend or revoke at any time. Breaches of this policy may be dealt with under the Behaviour Policy (students), Code of Conduct (staff and volunteers), and Terms & Conditions (parents). Serious matters will be referred to the police or other appropriate authorities.

Anyone using online services in a way that compromises the safety, security, wellbeing or respect of others may be deemed in breach of this policy.

The use of electronic and social media communication that violates the terms outlined in this policy, the staff code of conduct or any local or international laws, may result in serious consequences, including suspension, termination and/or police intervention.

IT: accessing the internet
Artemis provides staff, students, community members and visitors to schools with online access free of charge. Access to the Internet and to online resources at Artemis schools is subject to filtering and monitoring procedures that are reviewed regularly. Visitors must acknowledge Terms and Conditions before accessing our networks.

IT: email
All Artemis/YOURNAME staff and students receive email addresses which are to be used for education related business. This e-mail system can be monitored, and all email is subject to data retention policies. Email accounts are provided under the assumption that they will be used for work related purposes.

In particular, users are reminded that their access to their email account and its contents will cease when they leave Artemis/YOURNAME and the account is closed, but that Artemis may be required by authorities such as the data protection regulators to reopen and access closed accounts in line with our data retention policy, and disclose any information that might be relevant to a subject access request or similar investigation.

Users' attention is drawn to the contract of employment which outlines the terms of use of this account. Artemis staff are advised to manage their email accounts with a regard to the risk of breach and compromise. Any unusual or suspicious activity associated with email accounts, including but not limited to messages containing documents and hyperlinks from unknown senders, must be reported immediately.

IT: cloud-based collaborative tools and shared drives

Staff and students must take appropriate steps to ensure that material used or stored in collaborative tools is not shared with unauthorised persons, that editing privileges are not abused or extended to those for whom read-only access is more appropriate, and that all data processing via such tools is done in accordance with the principles of fair processing as defined and described in Article 5 of the General Data Protection Regulations.

Staff must take care to ensure that materials are appropriately accessible to relevant leaders to ensure continuity of care and operational efficiency.

IT: physical IT assets
Access to computers must be limited to students and staff who require access for the normal performance of their educational programme/job. Levels of access are set and confirmed by authorised personnel.

All losses and/or suspected compromises to device security should be reported to authorised personnel.

Computers and mobile devices holding special category data (as defined under the Data Protection Act, 2018 in the United Kingdom), or personal data of special nature should be secured in a locked room or facility during non-school/working hours.

Passwords are for personal use and should be kept secure. Students and employees must not give out their passwords to other students/staff, or to any person outside the organisation without appropriate authorisation. Students are permitted to share passwords with their parents or guardians.

IT: portable devices
Artemis employees and students who have been allocated a portable device are regarded as the device's owners for the duration of their employment or matriculation at Artemis/YOURNAME and are required to take reasonable care of their portable device at all times. Reasonable precautions must be taken to keep the device secure and to safeguard the information stored on it. Portable device owners are expected to be especially mindful of the danger of theft in public locations.

Artemis employees and students are referred to the terms and conditions attached to the portable device scheme and are reminded that Artemis may, at its discretion, require employees or students to meet the costs of any repairs or replacement against loss or damage that may arise from carelessness with their portable device.
The member of staff or student who is allocated a portable device is the person authorised to use that device and the software on it. They may not distribute user rights to another party. Data stored on the portable device must be backed up regularly as protection against theft or mechanical malfunctions.

Responsibilities of the Staff Member when using ICT

In accessing electronic communication systems and social media applications, it is expected that staff will:

1. Sign the Acceptable Use Policy (AUP) and Network Access Agreement, on an annual basis, in order to be given access to and use the school's electronic communication systems and understand that compliance is a condition of access.

2. Demonstrate digital citizenship, both during and outside of school hours, by conducting all related activities in a responsible, ethical, legal, and respectful manner in accordance with the staff of conduct and the AUP.

3. Advocate and model digital etiquette, responsible social interactions, and safe and ethical use of electronic and social media communication, including respect for copyright, intellectual property and the appropriate documentation of sources.

4. Practice safe online behaviour and report any inappropriate communication (i.e. distribution of information harmful to others or information regarding a potentially dangerous situation that may threaten the safety of others).

5. Protect access to their individual network account by the use of a private, personal password, ensure that their personal password is not shared, and agree not to use the password of any other individual.

6. Respect the privacy of others (i.e. students, staff, parents, and community members) including, but not limited to, the sharing of photos, videos, and personal information without informed consent.

7. Ensure that personal use of electronic communication systems neither interferes with, nor distracts from the duties and responsibilities of the staff member.