ACS Acceptable Use Policy

Please note:

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, ACS 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.

ACS is committed to inclusion across race, gender, faith, identity and abilities. We believe that diversity helps us to fulfil our purpose, realise our vision and exemplify our values.

Document Status

Document Name:	Acceptable Use Policy
Document Status:	Final
Document Owner(s):	Head of IT
Responsible:	Director of Education and Integrated Technology
Accountable:	Chief Executive, Board of Trustees
Consulted:	Heads of School, School-based IT leaders
Informed:	Designated Safeguarding Leads

Change Control

Date Produced	July 2024
Version	V 7.1
Status and Review Cycle	Non-statutory, Annual
Review Date	July 2025

Purpose

This Acceptable Use Policy outlines how we expect 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 school and work). Parents, students, staff, and visitors who do not acknowledge this policy in its latest version may be denied access to ACS IT resources.

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

This policy stands within a suite of related policies, particularly regarding Online Safety, Privacy, and Data Protection. It aims to:

- set guidelines and rules on the use of school IT resources for staff, pupils, parents 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 IT systems
- support the school in teaching safe and effective use of IT.

1 Definitions

IT 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 (SIS, LMS, VLE, VC), and any device system or service which may become available in the future which is provided as part of the organisation's IT services[1]

Users: anyone authorised by the school to use the school's IT facilities, Trustees, staff, students, volunteers, parents/carers, contractors, and visitors.

Personal use: any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

[1] Other examples include telephone, mobile phone, fax, audio visual equipment, lines, transmitters and receivers and data communications and processing systems (including wired and wireless devices, computers, workstations, laptops, iPads, PDAs, printers, servers, scanners, digital still and video cameras and other computer hardware and equipment, computer labs, software, licensing arrangements, data files and internal computer and communications networks) that can be accessed directly from ACS computer networks intranet, extranet; portable devices, fixed hardware and infrastructure; cloud-based servers and services.

Authorised personnel: employees authorised by the school to perform systems administration and/or monitoring of the IT facilities

Materials: files and data created using the school's IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

2 Guiding principles for acceptable use

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

- Be polite, do not be abrasive in your communication to others.
- Use appropriate language. Do not swear or use vulgarities or other inappropriate language.
- Note that the ACS Intranet is not a place where privacy can be guaranteed
- Privacy is difficult to assure in public-available platforms, and digital information is very difficult to remove/delete from devices and platforms
- Respect the intellectual property of other users and information providers.
- Respect the privacy of others with regard to use of images, video and other content.

3 Unacceptable use

Unacceptable use of the ACS IT facilities includes:

- using IT facilities to breach intellectual property rights or copyright
- using IT facilities (including any ACS 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 ACS
- breaching IT policies or procedures
- cyberflashing
- 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 the school, 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 ACS 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 ACS, its customers, suppliers, staff, students or volunteers

- unauthorised analysis or penetration testing of ACS technologies and digital systems (including wired networks, wireless networks, Bluetooth, AirPlay, Infrared and the wider Internet of Things), with or without intent to compromise security or violate privacy
- interception or interference with RFID/NFC communication, particularly abuse of identification and security infrastructure (e.g., skimming, spamming, emulating, cloning, and spoofing)
- use of any device or software intended to cause Low Frequency or Distributed Denial of Service attacks on ACS networks, mobile devices, or personal medical equipment.

This is not an exhaustive list. The Head of School or Director of Education and Integrated Technology will use their professional judgement to determine whether any act or behaviour not listed above is considered unacceptable use of ACS IT facilities.

Any exception to this policy must be approved in writing by the Head of IT or another member of the ACS Leadership Team.

4 Internet access

ACS provides staff, students, community members and visitors to the campus with online access free of charge. Access to the Internet and to online resources on ACS campuses is subject to filtering and monitoring procedures that are reviewed regularly.

Visitors must acknowledge ACS Terms and Conditions before accessing our networks. Long term contractors must contact the IT help desk for advice.

5 Email

All ACS staff and students receive ACS email addresses which are to be used for school-related business. ACS's e-mail system can be monitored, and all email is subject to data retention policies.

ACS 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 ACS e-mail account and its contents will cease when they leave ACS and the account is closed, but that ACS 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.

ACS 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 to the IT helpdesk.

6 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 business owners or school leaders to ensure continuity of care and operational efficiency.

7 Physical IT assets

Access to computers and computer rooms must be limited to students and staff who require access for the normal performance of their educational programme/job. Levels of access are set by ACS Leadership Team members or their designees, and confirmed by authorised personnel.

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

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 (as defined under Chapter 4, Article 16 of the Law No. 13 of 2016, Promulgating the Protection of the Privacy of Personal Data in Qatar), should be secured in a locked room or facility during non-school/working hours.

ACS publishes a separate Password policy. Passwords are for personal use and should be kept secure. Students and employees must not give out their passwords to other students/staff of ACS, or to any person outside the organisation without appropriate authorisation. (Under the Password policy ACS students are permitted to share passwords with their parents or guardians.)

8 Portable devices

ACS 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 ACS, 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.

ACS employees and students are referred to the terms and conditions attached to the ACS portable device scheme and are reminded that ACS 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 ACS 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.

9 Mobile phones and telephone/VOIP communication

ACS monitors its communication systems. ACS reserves the right to monitor the destination and length of outgoing calls where it has grounds to suspect serious or constant misuse. All ACS phones must be registered on our Mobile Device Management platform and linked to an ACS email address/ Apple ID.

Recordings and transcripts of conversations and meetings must be made and retained in accordance with UK law and ACS data privacy and retention policies.

ACS staff who are issued with mobile phones must

- ensure the security of the phone (and any allied equipment) at all times.
- use the phone responsibly, and reimburse costs incurred for any calls made for personal purposes
- remain up to date and informed about laws regarding the use of mobile phones (for example UK laws forbidding drivers from making or receiving calls or texting on a hand-held mobile phone whilst driving).

10 Distance learning

This policy extends to all distance, hybrid, and remote learning and working environments.

Synchronous lessons and personally-identifiable student learning artefacts used in remote learning may be recorded for educational purposes (for example, for other students to use after the lesson has finished), as well as for the monitoring and improvement of quality, subject to the ACS data privacy and retention policies.

Private tuition must not be facilitated using ACS devices. Instead, tutors must use privately owned devices and e-mail accounts when they undertake private tutoring. ACS publishes separate guidance for parents on private tuition, including staff good practice guidelines.

Participation in classes, meetings and conferences hosted online using video conferencing software is by invitation only. Unauthorised presence at such meetings will be considered

to breach the expectations of respect outlined in the Code of Conduct and Behaviour Policy.

11 Sanctions

All users must agree to comply with this policy as well as with other applicable laws, rules, policies and regulations. Access to ACS 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.

12 Social Media

In addition to requirements outlined in the Online Safety Policy and Code of Conduct, ACS provides separate guidance for staff use of social media.

13 Related Policies and Procedures

This policy is associated with and should be read in conjunction with the following ACS policies:

- Anti-bullying Policy
- Behaviour Policy
- Child on Child Abuse Prevention and Response Policy
- Data Protection and Retention Policy Suite
- Information Security Policy
- Online Safety Policy
- Password Policy
- Privacy Notice
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Whistleblowing Policy

All these policies are available on the ACS website at www.acs-schools.com or the policies page on Schoology.

Appendix

AUP Summaries and Required Acknowledgements

Staff

When using ACS IT facilities and accessing the internet in school, or outside school on an ACS 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 organisation's reputation
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, licences, or connect unauthorised hardware or devices to the school's network, or access unauthorised services (including digital platforms or subscriptions)
- 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 students or staff, or other members of the community
- Unethically use generative AI, or transmit sensitive and personally identifiable information to AI platforms
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses or conduct unauthorised transactions or commerce
- Treat ACS IT assets without due caution and reasonable care

I understand that ACS will monitor the websites I visit and my use of IT facilities, systems and devices. 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 ACS policies.

I will secure and take reasonable care of devices issued to me, including application of updates and general maintenance, and return them upon request.

I will let the designated safeguarding lead (DSL) and school-based IT leader know if a student or parent 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 ACS ICT systems and internet responsibly, and monitor that students in my care do so too.

I have reviewed the ACS Privacy Notice and Acceptable Use Policy.

I understand ACS Staff Use of Social Media Guidelines.

Parents/carers

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, ACS social media accounts, or personal social media to complain about or criticise members of staff. This is not constructive, and we can't improve or address issues unless they are raised in an appropriate way
- use private groups, ACS social media accounts, 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 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.

I have reviewed the Acceptable Use and Online Safety Policies.

I have discussed the Student Acknowledgement that summarises these policies with my child in an age-appropriate way, and I confirm that they understand what constitutes acceptable use of technology at ACS.

Students

When using the school's IT facilities and accessing the internet in school and when using my school-issued or my own device(s), I will not:

- Use them for any non-educational purpose
- Use them without a teacher's permission or instruction
- Use them to break school rules
  - Conduct unauthorised analysis or penetration testing
  - Intercept of interfere with RFID/NFC communication
  - Use any device or software to cause any Denial of Service attack on ACS systems or personal devices connected to ACS networks
  - Disrupt or interfere with IT services, or put ACS networks at risk
  - Modify device management settings
- Access any inappropriate websites
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online
- Share any semi-nude or nude images, videos or live-streams, even if I have the consent of the person or people in the photo/video
- Share my password with other students or log in to the school's network using someone else's details
- Bully, harass, or interact disrespectfully with other people
  - Unethically use generative AI, including creation of inappropriate text and images, as well as illegitimate or unacknowledged use in assignments
  - Bring the school or its staff into disrepute.

I understand that the school will monitor the websites I visit and my use of the school's IT devices, 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 devices, IT systems, and internet network responsibly.

I understand that the school can discipline me if I use technology unacceptably, even if I'm not in school.

Visitors

Stay connected while you explore our vibrant educational community! Whether you're a parent, visitor, or guest, we're delighted to offer you access to our high-speed internet. Please take a moment to read and agree to our terms and conditions before you connect.

Terms and Conditions:

1. The guest Wi-Fi service is provided solely for lawful purposes, including educational and personal use. Any illegal activities or attempts to access restricted content are strictly prohibited.
2. This service is intended for casual internet browsing and email. Streaming videos, downloading large files, or engaging in bandwidth-intensive activities can interrupt learning and business operations. Please be considerate.
3. Users are responsible for maintaining the security and confidentiality of their own devices. ACS will not be held liable for any loss or damage to personal devices or data.
4. The guest Wi-Fi service is offered as a convenience and does not come with technical support. We cannot guarantee the compatibility or availability of specific devices or applications.
5. The guest Wi-Fi is a limited service which is subject to filtering and monitoring; usage is logged for security and network management.

By connecting to the Guest Wi-Fi, you agree to comply with the above terms and conditions. Failure to adhere to these guidelines may result in the termination of your access.

SSID: ACS Guest Wi-Fi

Password: [Provided password]

Once again, welcome to ACS International Schools. You can read our Privacy Notice and Acceptable Use Policy online at www.acs-schools.com/policies.