ACS Acceptable Use Policy

Please note:

In countries where ACS International Schools is operating outside of the United Kingdom the UK regulatory framework will provide the foundation for best practice as far as this policy is concerned. All ACS schools will operate in compliance with the relevant legislation of the country in which they are operating.

ACS International Schools is committed to protecting individual's personal data, and aims to remain at all times fully compliant with data protection laws and guidance from the relevant regulators. ACS further commits to ensuring that the planning and writing of all policies and procedures that involve the handling of personal data are guided by the principle of privacy by design, and that individuals' rights to have their data safeguarded are a paramount consideration in ACS' pursuit of all its operational and strategic practices.

Document Status

Document Name:	ACS Acceptable Use Policy
Document Status:	Final
Document Owner(s):	Head of Central IT Compliance, Accreditation and Policies Officer
Responsible:	Compliance, Accreditation and Policies Officer
Accountable:	Chief Executive, Governing Board
Consulted:	Heads of School, Digital Teaching & Learning Coordinators, Online Safety Coordinators
Informed:	Designated Safeguarding Leads

Change Control

Date Produced	March 2020
Version	V6.1
Status and Review Cycle	Non-statutory, Annual
Review Date	March 2021

1. Policy Statement

1.1 ACS International Schools Ltd. (henceforward referred to in this policy as ACS), recognises the value of technology in supporting and enhancing teaching and learning and in facilitating school processes and systems. ACS provides and maintains technology to support the educational programmes and operations of the organisation. This policy describes and defines acceptable and appropriate use of technology, which includes but is not limited to, computer and information systems, networks, peripheral devices, telephone and fax equipment and other technology resources.

1.2 This policy applies to all technology owned or maintained by ACS, and to all users of, or connected to, this technology, whether on or off campus.

1.3 This policy and its appendices also set out guidelines for the use of social media for ACS students and employees, with the intention to provide a framework for those interested in establishing a social media platform on which to promote or celebrate ACS activities. In providing this framework, ACS is mindful of the responsibility all organisations have to safeguard their own reputations and the wellbeing of their community members within social media, and online in general.

1.4 In addition, this policy sets out acceptable and appropriate use of social media platforms where use of those platforms is either facilitated by ACS or is associated with ACS because of the use of ACS' name, logo or images identified with the school's campuses, personnel or products.

1.5 Anyone using ACS technology does so at their own risk. ACS is not responsible for any equipment damage or data corruption that may be suffered by the use of ACS technology.

1.6 As a condition of using ACS technology, all users 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.

1.7 All members of the ACS community are bound by the national laws relating to civil rights, harassment, copyright, data protection, security and other statutes relating to electronic media relevant to their location. This policy does not preclude enforcement under the laws and regulations of the relevant national authorities.

1.8 All members of the ACS community are expected to conduct themselves with regard to the responsibilities consistent with this policy and all other applicable ACS policies. Abuse of computing and/or network privileges may lead to disciplinary action, which may include summary dismissal.

1.9 Abuse of networks or computers at other sites through the use of ACS resources will be treated as though it occurred at ACS. When appropriate, restrictive actions will be taken by systems or network administrators pending further disciplinary or legal action which may include prevention of further use of ACS technology, blocking various access, removal of equipment or other security measures.

1.10 This policy is not intended to address each and every situation in which a safe practice matter that involves the use of online technology occurs. In the course of school activities it is normal for school administrators and other community members to expect all users of technology and online platforms to observe the ACS values and to respect others. Anyone using online services in a way that compromises the safety, security, wellbeing or respect of others may be deemed in breach of the guidelines contained in this policy, which is offered for the benefit of all ACS community members and reviewed annually.

2. Policy Guidelines

2.1 The ACS community is encouraged to make innovative and creative use of technology in support of education, research, academic development and internal administration purposes only. Commercial uses are specifically excluded.

2.2 All students and employees are responsible for ensuring that computer and communication facilities are used in an effective, efficient, ethical and lawful manner and in consideration of others. This policy is intended to respect the rights and obligations of academic freedom.

2.3 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)*, and with *Keeping Children Safe in Education (September 2019)* and *Annex C* of that same document. ACS acknowledges its duty of care over students and commits to following the Independent Schools Inspectorate's guidance as set out in *Handbook for the Inspection of Schools Commentary on the Regulatory Requirements (September, 2019) Part 3 – Welfare, health and safety of pupils, para. 151-2 p. 29.*

2.4 ACS is committed to its vision: through learning inspiring all to make a difference, and to its core values:

- we engage in community;
- we promote excellence through learning
- we drive positive change

- we enrich the international experience

ACS' Expected Schoolwide Learning Results extend to all community members and are embodied in the aims of this policy. ACS expects and believes effective learners, confident individuals and caring contributors to act with integrity and respect with regard to their use of technology. This policy is, therefore, to be viewed as extending from the ACS values.

3. Definitions

ACS Technology. The organisation's telecommunications systems including but not limited to 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.

ACS Intranet. An online platform on which information about each ACS school campus and the organisation as a whole is published. The ACS Intranet is accessed via user names and passwords provided to ACS community members.

Managebac. Managebac is used as a repository of IB teaching and learning resources.

Ownership and Access. In this policy, the terms ownership and access relate to use of computers and technologies that are the property of ACS and that are made available to user groups including: students (in support of their academic and student life objectives and requirements); employees (in support of their teaching, administrative functions or their assigned responsibilities); and other authorised users (in support of the authorised use of ACS technology).

Portable Devices. Laptop computers, iPads and similar devices that are designed to be lightweight and easy to transport. The fast-moving nature of this field of technology means that not all categories of portable devices can be named and identified, but reference to portable devices in this policy should be regarded as covering any device that is not intended to be used in a single fixed location.

PowerSchool Learning. As part of the process of replacing the ACS Intranet with PowerSchool Learning, ACS has made the PowerSchool Learning Virtual Learning Environment (VLE) available to users.

Users. All members of the ACS community including students, parents, employees, independent contractors, consultants, volunteers, temporary workers, visiting scholars and campus visitors.

4. Safe Usage

4.1 Access to computers and computer rooms must be limited to students and employees who require access for the normal performance of their educational programme/job. Levels of access will be decided by Digital Teaching and Learning Coordinators working in cooperation with principals/line managers and Central IT. All losses and/or suspected compromises to device security should be reported to the security staff.

4.2 Computers holding special category data (as defined under the GDPR), and mobile computers should be secured in a locked room or facility during non-school/working hours. Computer system security is the responsibility of all ACS staff and students, and is overseen by Central IT. Any suspected data security lapses on any system should be reported to the Coordinator of Digital Teaching and Learning and the Data Protection Officer.

4.3 All stakeholders should read and familiarise themselves with the Acceptable Use Policy. Occasional updates to the policy may be sent to the community via notices publicised at appropriate intervals.

4.4 Academic staff are responsible for ensuring that students understand what constitutes acceptable use of technology (including social media) and that age-appropriate explanations that students can understand and remember are given in lessons, on posters and other printed materials and in other forms determined at divisional level.

4.5 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/employees of ACS, or to any person outside the organisation without appropriate authorisation.

4.6 ACS recognises that staff members and students may sometimes find external software helpful in teaching or in facilitating their work. However,

the introduction of some software without appropriate care and understanding of what functions the software enables may compromise the safe use of ACS technology for other users, and increases the risk of introducing malware to ACS' systems and the risk of breaches of data privacy.

Staff members and students who wish to use external software, including mobile apps, beta programs and downloads must obtain prior approval from their appropriate line manager and final approval from the Head of Central IT. In most cases prior approval will be from the principal or the campus Coordinator of Digital Teaching and Learning.

4.7 The campus Coordinator of Digital Teaching and Learning may authorise teachers to download apps according to the teacher's professional judgement, and where the campus Coordinator of Digital Teaching and Learning is satisfied that there is no compromise to data privacy or online safety measures.

Where there is any doubt about the potential of software to compromise ACS' systems, security or other users, a referral should be made to Central IT by raising a ticket with the Helpdesk at helpdesk@acs-schools.com.

4.8 Misuse of Information Technology, computers, mobile devices and related equipment is a serious disciplinary offence and could lead to action being taken, up to and including dismissal from the organisation. The following is a non-exhaustive list of examples of misuse:

- Fraud and theft.
- System sabotage/introduction of viruses.
- Using unauthorised software.
- Obtaining unauthorised access.
- Breaches of Data Protection laws.
- Sending or forwarding any message via electronic mail that could constitute bullying or harassment (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.

5. E-mail

5.1 All ACS staff and students receive ACS e-mail addresses which are to be used for school-related business. ACS' e-mail system can be monitored in line with the ACS Data Privacy policy.

5.2 ACS is mindful that e-mail is known to be one way those wishing to do harm to children have made their initial contact and begun the process of grooming. ACS staff are, therefore, reminded of the need to be vigilant for signs of the potential misuse of e-mail.

5.3 ACS e-mail 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.

6. School Website and Intranet

6.1 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.

6.2 ACS will not tolerate the use of online access for illegal activities or for activities inappropriate to a school setting intended to be a safe place for learning.

6.3 Under no circumstances should ACS network security be circumvented using tools such as VPNs (virtual private networks), proxies or any other method of 'traffic tunnelling' designed to masquerade activity or locality unless specific authorisation is obtained from the Head of IT.

6.4 Displaying or downloading information or images that are offensive, obscene, abusive, objectionable or dangerous is not permitted. Sensitivity to the diversity of the ACS community will be considered in deciding whether or not material is offensive.

6.5 Using another person's password, or trespassing in another person's folders, work or files is not permitted.

6.6 Using the ACS Intranet for personal financial gain or personal commercial activity such as offers of products or services, etc., is not permitted.

6.7 All users are expected to abide by the following generally accepted rules of network etiquette:

- 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.
- 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.

7 Information Systems

7.1 In order to maintain the confidentiality of information on ACS' computer information systems, ACS employees and students are required to abide by all security measures established by ACS to safeguard information systems. These include, but are not restricted to, passwords, access safeguards and identification processes.

7.2 ACS employees and students are required to ensure they have appropriately secured their device's privacy when leaving them unattended. For example, by logging out of the ACS network or locking their device via a secure password.

8 Portable Devices

8.1 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.

8.2 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.

8.3 The ACS employee 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. Cloud-based Collaborative Tools and Shared Drives

9.1 ACS recognises and acknowledges the ubiquity of cloud-based tools such as Google Drive, OneDrive and so forth that are designed to facilitate collaborative work. ACS regards it as a professional expectation that contributors to documents shared via such services ensure the content they add is accurate and that it constitutes fair processing as defined and described in Article 5 of the General Data Protection Regulations. Among other things, this means acting to rectify any false information as soon as it is recognised as false.

9.2 When using such tools for school purposes, ACS expects users and

contributors to use professional judgement, and to abide by the relevant data protection legislation and ACS' own Privacy Notice.

9.3 In particular, ACS as a data controller expects its staff to recognise and abide by their 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. Among other things, this means taking appropriate steps to ensure data shared via such 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.

10. Distance Learning Tools

10.1 Like other schools, ACS employs various distance learning tools to ensure continuity of teaching, learning and essential business during times when the school may be closed owing to exceptional circumstances such as extreme weather or a pandemic. The AUP is deemed to cover these circumstances and normal site-based activities equally.

10.2 Students who engage in distance learning are required to indicate their understanding that lessons conducted online synchronously (i.e. live, at the time the lesson is taught by the teacher) may be recorded for the use of students learning asynchronously (i.e. later, after the lesson has finished), as well as for the monitoring and improvement of quality. The usual data privacy rights apply to such lessons, including data retention periods.

10.3 Faculty who are teaching in a distance learning forum are deemed to be working under the ACS Code of Conduct and all relevant policies regardless of their physical location at the time the lesson is taught.

10.4 In addition, faculty must abide by the Online Safer Practice Expectations for ACS students, Families and Teachers when teaching distance learning lessons. In particular, faculty's attention is drawn to the dress code associated with such lessons, the suitability of the location from which the lesson is taught and the safeguarding precautions required to be followed.

10.5 Distance learning lessons that involve one-to-one student-teacher arrangements must be appropriately risk assessed and signed off by the relevant divisional administrator (principal or assistant principal).

10.6 All considerations regarding behaviour and respect apply equally to online/distance teaching and learning and normal site-based teaching and learning.

11. Mobile phones and the ACS Telephone System

11.1 ACS monitors its telephone system on a regular basis. ACS employees are advised that ACS reserves the right to monitor the destination and length of outgoing calls where it has grounds to suspect serious or constant misuse of its telephone system.

11.2 ACS employees who are issued with mobile phones for use at work must ensure the security of the phone (and any allied equipment) at all times.

11.3 ACS employees are expected to use mobile phones that are issued to them responsibly and to declare and reimburse costs incurred for any calls made for personal purposes not connected with ACS business.

11.4 When agreed beforehand and approved by the appropriate line manager, employees who use their personal mobile for business purposes may be reimbursed for business calls.

11.5 ACS employees are expected to remain up to date and informed about national 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).

12. Prohibited Activities

12.1 ACS recognises the formal definition of malicious communication in the UK as sending a letter or electronic communication with intent to cause distress or anxiety.

12.2 Users shall not use ACS technology, directly or indirectly for illegal or inappropriate activities. Such activities include, but are not limited to:

- Creating, facilitating, or performing any illegal activity or violating the legal rights of others.

- Circumventing the user authentication or security of any device, host, network, application, or account (including hacking, breaking in, or stealing files or data) or using, disclosing, or changing another person's password, without the express consent of that person or the appropriate person in authority at ACS.

- Posting, transmitting, communicating, or disseminating content which violates the rights of others or which is unlawful, malicious, threatening, abusive, libellous, slanderous, harassing, defamatory, offensive or objectionable to a reasonable person.

- Uploading, downloading, posting, publishing, transmitting, retaining, reproducing, sharing, or distributing in any way information, software, movies, music, books, articles, or any other material which is protected by copyright or other proprietary right(s), without obtaining permission of the owner.

- Using any ACS-owned computer to access, post, transmit, or disseminate obscene or pornographic content.

- Copying, modifying, utilising, or sharing software in violation of a software licence.

- Restricting, inhibiting, or otherwise interfering with the ability of others to use or enjoy ACS technology, including generating levels of traffic sufficient to impede others' ability to send or retrieve information or wasting technology resources. This includes printing too many copies of a document or other unnecessary output; using networked resources for recreational purposes; and high-bandwidth activities such as uploading, downloading, or sharing software, music, video, and other media files whether through FTP, a centralised service, through peer-to-peer sharing or other arrangement for personal or recreational use.

- Diverting or intercepting network transmissions unless authorised to do so.

- Engaging in fraud, misrepresentation, "phishing," or falsifying addressing information to conceal, spoof, or mask a sender or recipient's identity.

- Using ACS technology for commercial purposes (other than ACS business) or unauthorised financial gain.

- Violating the policies of, or disrupting activities on computers and mobile devices used in school.

- 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, employees or students.

13. Privacy

13.1 ACS commits to respecting all privacy rights in keeping with its observance of the ACS Privacy Notice, national privacy legislation, the Data Protection Act, 2018 and the General Data Protection Regulations, 2018.

13.2 Within the bounds of these policy and statutory guidelines, and in accordance with all applicable laws, ACS may monitor the activities and communications of its users. For example, ACS may monitor the activities of students and employees when needed to investigate a possible disciplinary offence or violation of law or the ACS codes of conduct, or to help ensure the proper operation of ACS technology. All users agree to such monitoring through their use of ACS technology. If monitoring shows possible evidence of improper or illegal activity, such evidence may be turned over to ACS authorities and/or law enforcement officials.

13.3 Forensic online monitoring is carried out daily and weekly to enable ACS to appropriately safeguard students and ensure that all staff online use is compliant with the Code of Conduct.

13.4 Staff who appear in the forensic online monitoring report will be recorded in the first instance if the monitoring log indicates inappropriate content. The data will be reviewed and the member(s) of staff concerned will be alerted to the occurrence.

13.5 Staff who appear in the forensic online monitoring log repeatedly for

inappropriate content or appear in the log due to illegal or potentially harmful content will be referred to the Deputy Head of School and/or HR and if necessary the appropriate outside agency such as the safeguarding authorities or police.

14. Other Information and Procedures Supporting this Policy

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

- Anti-bullying Policy
- Behaviour Policy
- Online Safety Policy
- Child Protection and Safeguarding Policy
- Whistleblowing Policy
- Health and Safety Policy
- Privacy Notice
- Password Policy
- Curriculum Policy
- Information Security Policy

All these policies are available on either the ACS website at www.acs-schools.com or the policies page on PowerSchool Learning. Alternatively, copies may be requested by writing to rharrold@acs-schools.com

Appendix One: Social Media, Blogging, Social Networking and Messaging

ACS recognises the legitimate useful purposes a blog or a social networking or messaging platform may serve to showcase class activities, support students' learning, display student work, facilitate telecollaborative projects and so forth. Blogs from providers such as Weebly, WordPress, Wikispaces etc. may be linked to teacher pages on PowerSchool Learning provided the authors of such blogs are mindful of their responsibilities under the General Data Protection Regulations, national laws including copyright laws, and any statement by an ACS community member regarding the use of their personal image or, in the case of an ACS parent, the image of their child.

ACS acknowledges the ubiquity of social media and its potential to support and enhance learning. ACS also recognises that use of social media can be a distracting element in school learning activities. Divisional principals and Head Office department heads are expected to establish guidelines for respectively teachers and head office staff on the appropriate use of social media during working hours. The terms and conditions associated with each social media platform will normally constitute the first consideration with regard to its appropriateness for use in a given learning setting with children.

ACS recognises the growing importance and benefits of communicating through social media. As ACS' own activity on social media has grown – and as the social media activity of ACS' community members has grown, so a greater understanding and appreciation of the potential benefits of social media has developed. ACS recognises that students and staff may be interested in promoting their work to the online community through social media, and thereby becoming advocates for ACS.

ACS recognises that social media is a fast-changing category of online activity and that various social media platforms have risen to prominence in recent years, some of which have endured and some of which have faded to obscurity.

ACS recognises certain identifying characteristics of social media such as its user-generated aspect and the fact that its content is generally shared online.

ACS has established a number of official ACS social media channels on popular social media platforms including Facebook, Twitter, YouTube and Linked In. In addition, other social media tools in use across the organisation include blogs, micro blogs, wikis, chat rooms, online communities, and video platforms (such as Vimeo).

ACS takes social media responsibility seriously. All ACS social media accounts are considered official communication channels. It is a requirement that any ACS accounts (accounts that use ACS in the title and speak on behalf of ACS) are set up with the Marketing Department and run to profession standards, and that ACS is aware of who is representing the organisation via the social media. For this reason,

any staff member(s) wishing to become official account holders of social media platforms representing ACS are advised to contact the Marketing Department.

ACS advises all staff members who become official ACS account owners that they will be fully responsible for the management and content of the account. Social media accounts need regular monitoring and checking daily, including weekends, and out of hours by account owners to ensure that messages and posts can be responded to in a prompt and timely manner. ACS keeps a record of official accounts and spokespeople and monitors activity. Any social media accounts using ACS will be picked up through monitoring tools.

ACS' primary official accounts are listed below:

Twitter

@ACSintschools
@ACSEgham
@ACSCIM
@ACSHillingdon
@ACSDoha
@ACS_Cobham
@ACSPartnerships

YouTube

ACSInternational1 - Marketing

LinkedIn

ACS Alumni group – Alumni Relations Department
ACS company page – Advancement/Marketing

Facebook

Facebook.com/ACSCobham - Marketing
Facebook.com /ACSEgham - Marketing
Facebook.com /ACSHillingdon - Marketing
Facebook.com /ACSDoha - Marketing
Facebook.com /ACSAlumni – Marketing

WordPress

headsblog.acs-schools.com

Instagram

@ACSIntSchools
@ACSDohaSchool

ACS acknowledges that many social network sites require members to be at least 13 years of age. ACS requires all students to adhere to the terms and conditions and policies of these sites, including the minimum age requirements.

ACS students are personally responsible for the content that they post, share and respond to online. When posting online, all information is considered representative of the poster's views and opinions and may not be assumed to represent the views of ACS.

ACS strongly advises users to recognise that online postings and conversations are not private. ACS community members are warned of the potential consequences of sharing confidential information, internal school discussions or specific information about students, staff or other community members via social media.

Users of social media may not refer to ACS in the names of social media accounts, or use ACS logos or images that are associated with ACS unless the account is an official account approved by ACS.

ACS staff members are reminded of the inadvisability of friending students on social media. Staff are referred to the Online Safety policy and to the ACS Staff Handbook and Code of Conduct "*Working at ACS*" for further information. Staff are further reminded to respect the privacy of other staff members and other community members and their preferences regarding their social networks.

All ACS community members are reminded that the school's values are expected to guide all behaviour whether on or offline. Students are expected to follow all ACS policies when online, and to conduct themselves as if at school. ACS will work in partnership with parents to monitor behaviour that negatively affects our students or reflects poorly on the values of the organisation, and students may face consequences for behaviour that violates ACS' values and policies.

When posting, even on the strictest settings, community members should act on the assumption that all postings are in the public domain. Community members are reminded that in microblogging (Twitter etc.), comments made using such media are not protected by privacy settings.

ACS' users of social media are reminded that under no circumstances should offensive comments be made about students, parents, staff or ACS in general. If responding to someone with whom they disagree, ACS stakeholders are reminded of the importance of respectful language and of the need to ensure any criticism offered is constructive and not hurtful. Posts and comments should help, build and support the ACS community.

In the same vein, ACS community members are reminded not to comment on or

forward unsupported information such as rumours and to ensure that their profile and related content is consistent with how they wish to present themselves to colleagues, parents, and students.

ACS acknowledges that pictures and other content posted on social media are public and information can be shared beyond the control of the original poster. Students are taught to consider whether posted content would give an unfavourable impression of the poster to potential future viewers including friends, parents, teachers or future employers, or provide damaging material to persons ill-disposed towards the poster. Students are taught that although it is often technically possible to remove content from the Internet or make it hard to locate, it can often be extremely difficult to undo the damage that ill-advised posts hold the potential to cause.

ACS has a separate Password policy that is intended to provide guidance to community users on safeguarding access to their online presence in all forums including social media. ACS expects users of online forums to observe this policy. Users are required to keep passwords confidential and to change them regularly in accordance with the Password policy. Under the Password policy ACS students are permitted to share passwords with their parents or guardians.

ACS students are further advised not to give out personal information, (including, but not limited to, last names, phone numbers, addresses or exact birthdates) on social media, and to accept social network invitations only from people they know.

ACS publishes a separate Child Protection and Safeguarding policy that describes the support available to children and other community users if they feel unsafe online.

In addition, ACS publishes a separate Online Safety policy. Students who find themselves in a social media interaction where they feel threatened or unsafe are encouraged to tell a parent or trusted adult immediately and to report any difficulties or escalating situations that are associated with school-sanctioned use of social media to a teacher or principal.

ACS staff who are using a social media account that identifies them as a member of ACS are reminded of the professional expectations contingent upon them. The guidelines in Appendix Two of this policy are set out as advised good practice and should not be regarded as comprehensive. Social media is a fast-changing field of human activity and staff are expected to employ common sense and professional judgement in all their decisions regarding what they post on social media platforms, whether or not ACS is the subject of the post.

Appendix Two: Best Practice Guidance on Use of Social Media

Identification of Poster with ACS:

Staff may mention that they work for ACS and may discuss ACS and promote their work. However, they must make it clear that views expressed are personal and not those of ACS.

Staff should refrain from making reference to ACS, its employees, customer and suppliers on social media. Their name or social media handle/title should not contain ACS in any form. Only approved ACS accounts with approved ACS spokespeople are authorised to do this.

Staff should be alert to the beguiling nature of the informality associated with many social media platforms. They should exercise care in what they say and be alive to the possibility that what they post may quickly be shared to other parties outside the control of the original poster or governing legislation.

Integrity

Staff are expected to be transparent and state that they work for ACS. Their honesty will be noted in the social media environment. If staff members are writing about ACS or about a competitor, they are expected to use their real name, identify that they work for ACS, and be clear about their role.

Where staff have a vested interest in what they are discussing, they are expected to be the first to say so.

Staff are expected to post meaningful, respectful comments and to avoid posting spam or making remarks that are off-topic or offensive.

Staff are expected to stick to their area of expertise and to feel free to provide unique, individual perspectives on non-confidential activities at ACS.

When disagreeing with others' opinions, staff are expected to keep their comments appropriate and polite. If an online situation appears to be becoming antagonistic, staff are expected to handle the situation with professionalism. This may require consulting with a colleague or line manager or it may require disengaging from the discourse in a polite manner that reflects positively on both the staff member and on ACS.

Staff are expected to seek appropriate guidance from a line manager before participating in social media when the topic being discussed may be considered sensitive (for example an incident or crisis situation, or a situation involving an intellectual property or commercially sensitive dispute).

Staff are reminded that a swift an honest apology for any mistakes made in both consistent with professional expectations and provides a foundation for trust for future social media activity.

Defamation & Libel

On an online social network any comment posted is clearly linked to the poster and their profile. Users of social media need to carefully consider what they post and be mindful of other peoples' views and feelings. In legal terms, content posted on social media is usually covered by laws relating to libel and defamation.

Content posted on social media constitutes evidence which courts can consider and require to be disclosed for use in litigation. Such content may be used as a reference with regard to interviews or other career decisions. ACS staff are reminded that in recent years UK libel courts have been used to recover damages for libel against posters of comments, tweets and other content on social media that was ruled to be defamatory.

Guiding Questions for Users of Social Media when Reviewing Content Prior to Posting

Are you happy for this information to be in the public domain?

Is the content derogatory, defamatory, discriminatory or offensive in any way, or could it bring ACS into disrepute?

Are you representing yourself or ACS in a false or misleading way?

Are all statements true and not misleading, and can all claims be substantiated?

Does the post display common sense and common courtesy? For example, has permission been sought to publish or report on conversations intended to be private or internal within ACS?

Have efforts been made to be transparent and to avoid breaching ACS' Privacy Notice and/or legal guidelines for external communication?

If the content of the post involves ACS' competitors, is the post appropriately diplomatic, factually correct and accompanied by any necessary and appropriate permissions?

Are appropriate privacy protections in place for both the poster and ACS? Is confidential information involved, and if so how is it safeguarded?

Posting images at ACS

In accordance with the Online Safety policy, ACS staff may not upload pictures to any social media (including photo sharing platforms such as Instagram, Flickr and Pinterest) of clearly identifiable ACS students or staff members who have not consented (or, in the case of children, have not had their legal guardians consent) to have their images shared in this way. This includes images of single students and images of multiple students that include a student where consent has not been granted.

Where there is any doubt about which students or staff have consented to permit their image to be shared, (or, where appropriate, have had consent granted on their behalf), the poster must contact the appropriate divisional secretary or other administrator for details of which students do not have image permissions.

If there is continued uncertainty about permissions following reasonable steps to establish permissions, staff are advised not to use the image in question.

The photo-tagging tool on Facebook and similar/comparable technologies in any social media platform must always be disabled if using pictures of students.

Publicising events at ACS

Staff are required not to publicise school events on social media before they happen. ACS' policy is to promote events after they have taken place.

Exceptions include some parent organised events that do not take place on campus, or events which Principals or Heads of School have agreed may be promoted beforehand.

In case of doubt, staff are expected not to promote the event, or to check with an appropriate line manager or with the Marketing Department.

Monitoring/Regulation of Social Media

Staff are expected to understand and recognise that social media is an interactive form of communication. It is expected that users will monitor their accounts and respond as necessary on an ongoing basis. This includes remaining watchful for security breaches.

Staff are expected to remain educated about risks to social media accounts, and in particular the dangers associated with accounts being compromised by an external attack or hack. Staff are advised to exercise care clicking on unidentified links in social media channels. Staff are also expected to block spammers and users who are abusive or inappropriate.

Divisional principals and Digital teaching and Learning Coordinators offer support at ACS for any staff member who experiences difficulty or who finds themselves in an escalating situation as a result