ACS
INTERNATIONAL
SCHOOLS

ACS Online Safety Policy

Please note:

ACS International Schools is committed to protecting individuals' personal data, and we aim always to remain 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.

ACS is committed to inclusion across race, gender, faith, identity and ability. We believe diversity enhances our potential to fulfil our mission.

Document Status

Document Name:	ACS Online Safety Policy
Document Status:	Final
Document Owner(s):	Group Online Safety Lead
Responsible:	Director of Education and Integrated Technology
Accountable:	Chief Executive, Governing Board (delegated to Education Committee)
Consulted:	Heads of School, Online Safety Group, Head of IT, Head of Boarding, Group Safeguarding Lead, School Technology Leaders
Informed:	Designated Safeguarding Leads

Change Control

Publication Date	**August 2025**
Version	**4.7**
Status and Review Cycle	**Statutory, Annual**
Next Review	**August 2026**

1. Introduction

Purpose. This policy provides guidance to ACS community members (staff, students and parents) about safe and responsible practice when using online resources. ACS takes seriously its safeguarding responsibilities, and it recognises that material accessed online can be a source of distress and harm as well as the source of enhanced learning.

Scope. This policy, and the associated use of the term “online safety” is intended to cover the Internet and devices with the capability of connecting to it, as well as all online platforms and resources. Its scope extends beyond school days and premises, encompassing what happens off-site and outside school hours. As with all other aspects of safeguarding, online safety is seen at ACS as a whole-school issue and responsibility.

Offsite use. Heads of School will take account of the behaviour of students when they are off the school site and disciplinary penalties may be imposed in line with school policies for inappropriate behaviour. This includes incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, and are linked to or may adversely affect the school and its community members. ACS reserves the right to search electronic devices and delete data in line with statutory guidance. We will deal with such incidents within the ACS Behaviour and Anti-Bullying Policies. Where incidents of inappropriate online safety behaviour that take place out of school come to our attention, we will inform parents/carers. We will also notify the relevant authorities if incidents away from school reach our criteria for reporting serious online safety concerns.

2. Regulatory framework

ACS International Schools Ltd. (henceforward referred to as ACS) was informed in the creation of this Online Safety policy by the guidance set out in the following documents:

Independent School Standards
Boarding Schools: National Minimum Standards
Keep Children Safe in Education
Prevent Duty Guidance (England and Wales) 2023
Data and Computer Misuse Act 1990
Voyeurism (Offences) Act 2019
Data Protection Act 2018
Online Safety Act 2023
Searching, Screening and Confiscation in Schools
Meeting digital and technology standards in schools and college (2023)

Further documents for guidance and key reference frameworks are noted in an appendix.

3. Intent

Safe online practices are an integral part of the skillsets of the learners who will shape the future, and schools have a key role to play in promoting the ethical behaviour of all those who engage in online activity.

ACS recognises the importance of balancing online safety with the benefits technology brings to learning, teaching and educational administration. Appropriate online activity can support the development of personal identity, sustain dynamic communities, particularly for international students, provide recreational opportunities, offer an authentic platform for creative expression, and develop global competence.

We also acknowledge that technology provides a potential platform from which those with intent to harm or exploit children can act. We understand that online technologies have increased the incidence of child sexual exploitation, impacted body image and self-perception, radicalisation and sexual predation. Online environments can easily become venues for bullying, child-on-child abuse, harassment and similar anti-social behaviour that fall within the scope of this policy.

This policy is not intended to address every situation and scenario involving online safety practices. However, we expect all users of technology and online platforms to act in line with ACS values. Anyone using online services in a way that compromises the safety, security, wellbeing or respect of others may be in breach of this policy and subject to disciplinary consequences.

4. Principles of Online Safety

4.1 Categories of risks. ACS's online safety is informed by the need to safeguard our community from four categories of risk described in Part Two of Keeping Children Safe in Education 2022*:*

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users;
- conduct: personal online behaviour that increases the likelihood of, or causes, harm
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

4.2 Key concepts. Our Online Safety Policy aims to promote effective lifelong digital citizenship, digital wellness, and digital literacy.

Digital citizenship. Online presence plays a vital role in the personal and professional lives of many people. Use of the Internet and online resources comes with responsibility to observe safe practice and to engage appropriately with published material and with other users. All community members should be aware of the dangers of using the Internet and online resources and how to conduct themselves online. We provide reasonable access so that students can develop age-appropriate knowledge, skills and attitudes about online safety.

Digital wellness/ Digital flourishing. Understand the benefits and dangers of online interactions, including the importance of developing empathy and perspective, creating positive digital footprints, and taking proactive stance against cyberbullying and other negative behaviour online; physical and mental health; self-care; How to keep talk "safe" and positive online; building healthy relationships and caring communities; positive and negative effects on developmental, emotional, physical and social wellbeing; self-harm; digital challenges and hoaxes (see Appendix).

Digital literacy/literacies. Digital literacy is the "ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills" (US National Library Association). Other terms for this future-oriented competency include multiliteracies, new literacies, and technology literacies (see Appendix).

Digital resilience. Digital resilience is a dynamic personality asset that grows from digital activation, i.e. through engaging with appropriate opportunities and challenges online, rather than through avoidance and safety behaviours.

4.3 Vulnerable students and protected categories. We recognise the potentially vulnerable position of students with special educational needs, as well as students and staff with protected characteristics under The Equality Act 2010.

Online safety incidents involving students with special educational needs require consultation with SEN (Special Educational Needs) case managers, and risks associated with student disabilities must be assessed and mitigated.

Bullying and abuse will be subject to disciplinary action under the Behaviour Policy or Staff Code of Conduct. Abuse that demonstrates or is motivated by hostility based on race, religion, disability, sexual orientation or transgender identity may be reported to the relevant authorities as a hate crime at the discretion of the DSL or Head of School, and in line with reporting thresholds established by UK local authorities.

5. Roles and Responsibilities

5.1 Whole school approach. ACS recognises that all staff have a role in the safeguarding of children in our care. Designated Safeguarding Leads (DSLs) and Deputy Designated Safeguarding Leads (DDSLs) are appointed in all campuses at ACS to provide leadership of safeguarding that is guided by an enhanced level of training in safeguarding and child protection, including specialised training in online safety. All staff at ACS are informed during induction who the DSLs are at the respective campuses and what they should do if they suspect there is a safeguarding concern.

The following section outlines the online safety roles and responsibilities of individuals and groups. This list is not exhaustive.

5.2 Trustees. The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online. The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- reviewing filtering and monitoring provisions at least annually;
- blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- having effective monitoring strategies in place that meet their safeguarding needs.

Trustees must ensure that online safety is a running and interrelated theme in safeguarding and related policies and procedures. This includes oversight of planning the online safety curriculum, training, and allocating roles and responsibilities that is delegated to the Heads of School

Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the Board has taken on the role of Online Safety Trustee which includes:

- regular meetings with the Online Safety Group
- annual review of monitoring of online safety and incident log, and any actions required by DSLs, Trustees, or school leaders
- contributing to semi-annual Safeguarding Trustee meetings and reports.

5.3 Online Safety Group. The Online Safety Group provides a consultative forum with representation from the school community, with responsibility for advising the Leadership Team on issues regarding online safety. The group is also responsible for regular reporting to the Group DSL and Director of Education. The OSG is responsible for:

- compliance with relevant laws and statutory guidance
- annual review/monitoring of ACS Online Safety Policy; filtering provision and policies; staff training for online safety
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth, progression and collection/evaluation of evidence from assessment that monitors the impact of digital safety initiatives
- consulting stakeholders – including parents/carers and the students about online safety provision, and providing for student voice and agency
- monitoring improvement actions identified through use of the 360 degree safe self-review tool
- promoting allied leadership across the group that promotes common excellence in online safety.

5.4 Head of School and School Senior Leadership Teams. The Head of School has a duty of care for ensuring the safety (including online safety) of members of the school community. Heads of School must

- be aware of the procedures to be followed in the event of a serious online safety allegation being made against staff, students or parents
- ensure that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- work with ACS group services to manage and protect ACS digital platforms, online services, and public reputation
- oversee delegated approval of online content to divisional principals or their appointed representatives
- appropriately inform the school community about online safety incidents and how they have been addressed
- communicate online safety expectations to parents, in collaboration with the PSO
- establish guidelines for staff on the appropriate use of social media during working hours
- ensure effective planning, provision, integration, and review of the online safety curriculum.

5.5 Designated Safeguarding Lead. Details of the school's designated safeguarding lead (DSL) and deputies are set out in our Safeguarding and Child Protection Policy, as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- supporting the Head of School in ensuring that staff understand this policy, and that it is being implemented consistently throughout the school
- working with the staff to address online safety issues or incidents
- managing all online safety issues and incidents in line with the school Safeguarding and Child Protection Policy
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- updating and delivering staff training on online safety
- liaising with other agencies and/or external services if necessary
- providing semi-annual reports on online safety in school to the Heads of School, Director of Education and Trustees.

The Group DSL supervises our Group Online Safety Lead (see job description in appendix).

5.6 School Online Safety Lead. This role convenes a school Online Safety Advisory Group and shares day to day responsibility with the Head of School and DSL for online safety issues, including a collaborative role in implementing online safety policies. The designated Online Safety Lead:

- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff, and documents student educational events

- receives and shares reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets with the ACS-wide Online Safety Group (twice each year)
- Collaborates with IT technical staff to ensure that required online safety technical requirements are applied in context.

5.7 Technical IT staff. ACS provides network security and online safety resources implemented by IT professionals. Technical IT staff must:

- keep up to date and communicate technical online safety information to the Leadership Team and ACS staff
- implement network/internet/digital technology monitoring solutions
- provide secure access to ACS networks that is safe and fit-for-purpose
- manage ACS devices issued to students and staff and implement IT policies.

5.8 Academic staff. All teaching staff and school leaders must have an up-to-date awareness of online safety matters and of the current Online Safety Policy and practices, and complete required training. All staff are required to:

- read, understand, acknowledge and follow the Acceptable Use Policy and Staff Code of Conduct
- report any suspected misuse or problem to their line manager, divisional principal or DSL
- ensure that all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- embed safety issues in all aspects of the curriculum and other activities
- guide students to sites and digital resources that have been checked as suitable for their use, and deal appropriately with any unsuitable material that is found in internet searches
- supervise students when they are using technology and/or online materials during school hours, with supervision that is suitable to their age and ability.

5.9 Students. Students must:

- understand and follow the Online Safety Policy and Acceptable Use Policy, including the misuse of Virtual Private Networks (VPN) and other technologies intended to circumvent ACS internet filtering and monitoring
- report abuse, misuse or access to inappropriate materials
- use personal mobile devices and digital cameras appropriately, including following policies on the taking/use of images
- understand the importance of adopting good online safety practice when using digital technologies both inside and outside of school
- understand this policy covers their actions both in and out of school, if those actions relate to, involve or affect the school community, other ACS students or staff or have the potential to do so

- accept responsibility for personal devices used on campus, including the existence and use of previously downloaded harmful content as well as inappropriate material accessed via technologies that bypass ACS filtering and monitoring systems.

We expect students to engage meaningfully with the Online Safety curriculum, act responsibly, and learn how to help peers who need to disclose online safety concerns. ACS welcomes student voices, and we listen to student experiences and concerns in a variety of ad hoc, curricular, and organisational conversations.

5.10 Parents/carers. Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Users who access ACS digital systems will be expected to acknowledge and follow the Acceptable Use Policy. We strongly encourage and expect parents to promote good online safety practice at home (including safety settings on students' personal devices), to talk with their children about how to use personal devices appropriately at school, and to model appropriate use of:

- digital and video images taken at school events in accordance with school expectations
- access to Student Information and Learning Management Systems
- respectful engagement on social media.

In their own use of ACS and external digital platforms, parents are responsible for

- acting as gatekeepers for their children's personal mobile devices use of on-line material and content, including provision and monitoring of systems to prevent students from accessing mature (18+) content online
- respecting the privacy of other students and their families, and ACS staff (especially during school disciplinary or police investigations)
- working in partnership with the school to monitor online behaviour that may negatively affect our students or reflect poorly on the values of the organisation
- not commenting on or forwarding unsupported information
- ensuring that their profile and related content are consistent with how they wish to present themselves to ACS staff, parents, and students.

6. Managing Online Safety

6.1 All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet. The DSL has overall responsibility for the school's approach to online safety, with support from school and group staff, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL will liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

6.2 The importance of online safety is integrated across all school operations by:

- staff and Trustees receive regular training (see appendix).
- a dedicated Group Online Safety Lead role supports the Group DSL

- regular staff email updates regarding online safety information and any changes to online safety guidance or legislation
- online safety integrated into learning throughout the curriculum
- assemblies and boarding house meetings conducted regularly on the topic of remaining safe online
- regular educational events and meetings with parents and ACS parents organisations.

7. Handling Online Safety Concerns

7.1 Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

7.2 Confidentiality will not be promised, and information may be shared lawfully. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully with appropriate support provided to the victim.

7.3 Concerns regarding a staff member's online behaviour must be reported to the Head of School, who will decide on the best course of action in line with the relevant policies including the Staff Code of Conduct and Disciplinary Procedure. If the concern is about the Head of School, it must be reported to the Chief Executive.

7.4 Concerns regarding a student's online behaviour must be reported to the DSL, who will investigate concerns with relevant staff members and manage concerns in accordance with relevant policies. Where there is a concern that illegal activity has taken place, the school will contact the police, where it is considered appropriate to do so, exercising appropriate professional judgment and avoiding unnecessarily criminalisation of student behaviour in line with Outcome 21.

7.5 For any reports on ACS-managed devices, safeguarding reports submitted after hours will be addressed on the next school day.

8. Online safety hazards

8.1 Online Bullying (also known as Cyberbullying)

ACS treats online bullying the same way as bullying carried out in person. In many cases, online bullying can be worse. Technology can powerfully enable anti-social behaviour such as verbal bullying, incitement to violence, exclusion, and non-consensual dissemination of images (including revenge porn and distribution of youth-produced sexual images, including 'deep fakes' and digitally manipulated images), as well as hurtful gossip, slander and libel.

Cyberbullying can often be especially hurtful because it violates traditional notions of safe space and can continue beyond the physical proximity of the perpetrator.

Online safety education curriculum includes clear instruction that online bullying is wrong, and it urges students to report/disclose such misuses of technology.

8.2 Child-on-child abuse and harassment

Online tools can be used to perpetrate abuse. In practice, behaviour and experiences in online space will often profoundly affect students' behaviour and experiences in school, at home, and in the community. Sexual violence and sexual harassment exist on a continuum and may overlap.

Sexual violence, sexual harassment and harmful sexual behaviour can occur

- between two children of any age and sex or gender identity
- within a group of children using online tools to make or carry out threats of actual sexually assault, or to sexually harass a single child or group of children
- through online and offline actions (both physical and verbal), including youth-produced sexual imagery.

We take victims of abuse and harassment seriously. Following a report, the DSL will make an immediate risk and needs assessment on a case-by-case basis in order to provide the victim(s) and the (alleged) perpetrator(s) appropriate support. Because young people often first disclose abuse to their friends, we educate students about how to provide appropriate support to peers, including clear guidance that they should talk to a trusted adult at home or in the school, and where they can go for further advice.

8.3 Other serious threats to online safety. Rapidly changing technology and commercial developments continually introduce new concerns about digital safety. Non-exhaustive examples of ongoing danger to children arise from:

- Grooming and exploitation
- Child sexual exploitation and child criminal exploitation
- Radicalisation (including but not limited to violent or extremist organisations; terrorism; far-right, racist, white supremacist, neo-Nazi and incel groups)
- Poor mental health (self-harm, body dysmorphia, eating disorders)
- Online hoaxes and challenges
- Online gambling
- Sextortion (online sexual coercion and extortion of children)
- Cybercrime.

8.4 General Artificial Intelligence. Generative artificial intelligence (AI) tools are now widespread and easy to access.

AI has potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. ACS will treat any use of AI to bully students in line with our Anti-bullying policy and Behaviour policy.

Creating, sharing or publishing AI-generated or augmented content that is not age or workplace appropriate is strictly prohibited by students and staff, and subject to a disciplinary response.

Artificial Intelligence technologies raise a wide range of other online safety issues, including

- Data privacy
- Harmful, inaccurate or biased responses
- Misinformation
- Academic integrity
- Gaps between current regulation and safeguarding guidance
- Inappropriate or illegal content, contact, conduct and commerce.

8.5 Harmful content. ACS filtering systems aim to prevent access to harmful content to these and other categories:

Discrimination	promotes the unjust or prejudicial treatment of people with protected characteristics under the Equality Act 2010
Drugs	substance abuse displays or promotes the illegal use of drugs or substances
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance
Malware/ Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography	displays sexual acts or explicit images
Piracy and copyright theft	includes illegal provision of copyrighted material
Self-harm	promotes or displays deliberate self-harm (including suicide and eating disorders)
Violence	displays or promotes the use of physical force intended to hurt or kill

9. Education about online safety

9.1 Digital literacies are an integrated aspect of all subject area curricula, including PSHE (Personal Social Health and Economic) and R(S)E. Online safety education is monitored for effectiveness, evaluated, and updated as appropriate (see Appendix- curriculum).

9.2 Parent education opportunities for online safety education are held at least annually. ACS facilitates access to trusted organisations and resources that can help parents keep children safe online (see Appendix- parent resources). Parents have access to National Online Safety resources from the National College.

10. **Group Services IT Provision**

10.1 Internet Access ACS provide access to the internet through managed networks for staff, students, and visitors. We use role-based identities, time and location to assess risk and grant appropriate levels of access (including boarding staff and students, who have additional access privileges).

10.2 Network security. ACS monitors network connections and usage from all devices accessing the internet through our networks. User identities are verified, and all incoming and outgoing traffic is assessed to restrict access to harmful content. In addition to next generation firewalls, we employ a range of security information and event management strategies.

10.3 Filtering and monitoring. ACS uses industry standard solutions to filter internet traffic and log individual user actions. Logs are regularly reviewed and may trigger real-time alerts that initiate pastoral interventions or disciplinary proceedings. Individual user data is retained in accordance with ACS data retention policies.

ACS aims to block harmful and inappropriate content, without unreasonably impacting learning and teaching. We take a developmental approach, with special attention to children under 13 whose access to general internet platforms (such as YouTube) is restricted.

Student use of ACS iPads on private networks, including home networks, does not have the safeguards provided by the school's filtering and monitoring system. When ACS iPads are used at home, physical controls are essential. Students should use ACS iPads in common areas, under adults supervision. Home networks should have parental controls enabled which apply age-appropriate filters. Parents should be aware of the limits of these controls in a rapidly changing technology landscape.

10.4 ACS accounts and email. Staff and students are given approved school email accounts. Prior to being authorised to use the email system, staff and students must agree to the Acceptable Use Agreement.

Personal email accounts are not permitted to be used for school communications. Any email that contains sensitive or personal information may only be sent securely via encrypted email. Staff are not permitted to communicate with pupils or parents via personal email accounts.

Staff members and pupils are required to report junk/phishing messages. The school's email system is configured to reduce threats from emails and attachments. Incoming and outgoing email is protected by a security platform that continuously assesses human risk and dynamically adapts policy controls, proactively defending against advanced phishing attacks and outbound data breaches.

Multi-Factor Authentication is enforced for all staff accounts, and staff receive regular cyber security-awareness training. Any cyber-incidents are managed in line with the Data and Cyber-security Breach Prevention and Management Plan.

10.4 Learning Management Systems and Virtual Learning Environments. Digital learning services at ACS have limited access with strict identity management. User actions are logged and monitored.

10.5 Educational technologies. ACS manages educational technologies accessed through our networks or installed on our devices. Staff have limited authority to download applications, and software purchases (including cloud-based applications) must be approved. ACS supports educational technologies that meet ICO standards for age-appropriate design for online services.

10.6 Video-conferencing platforms. ACS centrally licenses and monitors access to communication platforms. We control enterprise settings in line with formal risk assessments for student user cases. We require students and staff to use approved platforms that have strong identity management, security and safety provisions.

10.7 Device Device Management. ACS is transitioning to fully-managed devices that allow greater visibility and control of user behaviour and online access. We have risk assessment in place to mitigate the more limited control of online access for students using ACS iPads or their own devices on our BYOD network.

11. Devices

Personal Mobile Phones, Tablets and Other Portable Devices

11.1 ACS provides appropriately filtered online access to all community members and to visitors to its campuses. Access by standard data contracts gives unrestricted access to web content that might be inappropriate, upsetting or disruptive in school settings. The unsupervised use by students of technologies (such as 3/4/5G wireless access or Virtual Private Networks) in order to bypass ACS' filtering and monitoring system is not permitted on campus, school transport or school trips.

11.2 Visitors' use of ACS online access services for the viewing, downloading or distribution of material that is violent, pornographic, otherwise offensive, or contrary to ACS values will be deemed reason for the removal of the right of online access, and may lead to a requirement that persons remove themselves, or be removed, from ACS premises.

11.3 ACS community members are informed that ACS filters and monitors web traffic in accordance with our statutory duties outlined in *Keeping Children Safe in Education*. ACS maintains a log of attempted access to blocked sites, and this log is maintained securely in accordance with the ACS Data Protection policy, the ACS Data Retention policy, and the ACS Acceptable Use policy.

11.4 Personal devices must not be plugged in to ACS wired networks.

11.5 ACS is not responsible for personal devices or services that provide passive location information about students, or for the accuracy of child tracking technologies. We encourage users to be aware of geolocation technologies and applications employed by personal devices and mindful of concerns they may present about safety, security, and consent.

11.6 BYOD policies. While we transition to fully-managed devices for high school students, ACS does not implement specific security policies for other student devices used to access our networks. However, we strongly recommend that devices using the BYOD network employ strong passwords and screen lock technologies. We advise BYOD users to use good judgment about personal and other sensitive data on devices that they use in school.

Personal computers and tablets (including search histories and downloaded files) are subject to the same disciplinary policies as students' personal mobile devices.

11.7 Managed devices. ACS provides iPads to students in primary and middle school (through Grade 8). We work with parents and our device management partners to provide safeguards and increase awareness of device controls. ACS is moving to a fully-managed estate for student devices in Grades 9-12, which will provide additional security and online safety measures.

11.8 Students in certain situations may be permitted to use mobile phones. Students in upper divisions have access to ACS digital assets and the internet through their own devices. All use of digital devices is guided by the separate Acceptable Use Policy.

School-owned Devices

11.8 Staff members may be issued with devices such as laptops, tablets, mobile phones or cameras to assist with their work. Students are provided with school-owned devices as necessary to assist in the delivery of the curriculum. School-owned devices must be used in accordance with the acceptable use agreements. School-owned devices are vvia a Mobile Device Management (MDM) Solution, and they must be password protected. IT technicians monitor school-owned devices and automate the installation of software updates and antivirus definitions. Prior authorisation from IT is required before any software, apps or other programmes can be downloaded onto a school-owned device.

Cases of staff or students found to be misusing school-owned devices will be managed in accordance with ACS Disciplinary Procedure or Behavioural Policy.

11.9 ACS laptop computers have encrypted hard drives. All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- keeping the device password secure
- maintaining appropriate device screen lock settings
- not sharing the device with family or friends.

Work devices must be used solely for work-related activities. Files stored on ACS devices are subject to review and deletion.

12. Online safety for classroom learning

12.1 ACS limits exposure to online threats accessed through our networks to the extent reasonably possible, in line with our duty of care to students, staff and visitors, as required by law, and in line with good practice standards from authoritative organisations. No filtering system can be 100% effective and must be supported with good teaching and learning practice and effective supervision.

12.2 ACS filters and monitors online content to ensure that it is appropriate for the age and maturity of students engaging with it. Staff may request access to websites or online services that would normally be excluded under terms of acceptable use, for approved instructional purposes. Divisional principals, or their delegates, are responsible for approving restricted sites and services in consultation with the DSL or Group Online Safety Lead. If a restriction is removed, safeguarding risks must be managed appropriately.

13. Public-facing digital systems (Including Use of Images and Video)

13.1 The ACS website at http:/www.acs-schools.com and our intra/extranet sites are key platforms on which ACS schools publish news and promote activities, programmes, events and student achievement. The platforms, even when password-protected, are public spaces. Uploaded content may be accessed by other members of the ACS community, and in some cases, the public.

13.2 ACS prohibits the use of children's full names alongside photographs published on any ACS platform or service. No combination of personal data that might allow an individual child to be identified may be uploaded; however, generic information such as class names or grade levels may be used.

13.3 Parents may withhold consent for their child(ren)'s image to be used in any publicly accessible space. Under the Data Protection Act 2018, children from the age of 13 up may give, withhold or withdraw their own consent independently of their parents' wishes. Staff must ensure that images and video are used on online forums has the appropriate permission.

13.4 ACS staff also have the right to withhold consent for their image to be used. Staff should consult the ACS Privacy Notice and discuss their wishes with their line manager and school marketing staff.

14. Social media

14.1 Use of social media at ACS is guided by the Acceptable Use Policy and Staff Guidelines for Social Media.

14.2 Criminals seeking to harm children have exploited weaknesses in social media platforms' inherent safeguards (such as the ease with which anonymity or disguise is facilitated) to gain the trust of children and begin the process of grooming.

14.3 ACS staff members may not friend students or otherwise associate with students on personal social media platforms (except for staff members communicating with their own children or family members, including those relationships such as godparent that carry a recognised special significance). When communicating with students or recent graduates for professional purposes, on approved web-based platforms or in e-mail messages, staff must not communicate in ways that might be misconstrued, including memes, images, or emoticons that can be misinterpreted. In some cases, such communications may constitute a criminal offense.

14.4 ACS values the continuing association many alumni wish to maintain with ACS following their graduation. This is formally recognised through the activities of the Alumni Relations Office, which include various social media groups. Staff are welcome to join ACS's social media groups and to engage with ACS alumni community through these channels. Social media contact on any platform between staff members and alumni younger than 21 years old is not appropriate, with the exception of professional contacts on LinkedIn for graduating students.

14.5 ACS expects staff and students to maintain positive online profiles and to be vigilant in monitoring their digital footprints. In admission and recruitment/hiring, applicants' public digital profiles are subject to review. Good practice includes:

- always promoting oneself, the school, school staff, parents and other students positively
- building a reputation that shows you at your best for education, work and life
- checking what online profiles says to universities, employers, friends and family
- communicating respectfully and appropriately.

14.6 ACS actively monitors its social media accounts and its online reputation.

15. Managing emergent technologies

15.1 ACS recognises that technology is a fast-moving field of activity and innovation. ACS risk-assesses novel technologies as appropriate, considering potential learning benefits as well as the potential exposure to digital safety threats. Digital innovation and pioneering modern technologies can present both exciting opportunities and significant safeguarding challenges. We take a collaborative approach informed by professional judgment of IT and education professionals to introduce, trial, and adopt emergent technologies.

15.2 Generative AIs in particular poses risks that must be managed by teachers and young people who are enthusiastic about their practical applications. Increased sophistication of deep fakes, scams, and misinformation; important debates about intellectual property rights, academic integrity; and difficult to monitor age-inappropriate materials/platforms demand critical thinking, engaged conversation, and ethical reflection by the entire school community.

15.3 Portable hacking tools can spoof, intercept, or interfere wireless communications. They are strictly prohibited under ACS's Acceptable Use policy. Digital safety encompasses student and staff responsibility for the physical security of RFID cards and identification technologies (such as facial recognition and passwords), as well as management of connected devices and the data they share with the Internet of Things IoT).

16. **Distance and hybrid learning**

16.1 ACS recognises that learning and teaching online can increase threats to students' safety and wellbeing. We risk assess online teaching and learning modalities to safeguard students and promote good practice. Distance learning, including livestreamed lessons, can only be delivered through approved platforms in accordance with ACS guidelines.

16.2 In distance and hybrid learning scenarios, we require that students and staff

- Complete a formal Remote Learning Risk assessment
- communicate within school hours as much as possible (or hours agreed with the school to suit the needs of staff)
- communicate through school channels approved by the senior leadership team
- use school or college email accounts (not personal ones)
- manage 1:1 interaction with appropriate supervisory notice and access
- use school devices wherever possible
- refrain from sharing inappropriate personal information.

16.3 Teachers should find a quiet or private room or area to deliver lessons or talk with students, parents or carers. When broadcasting a lesson or making a recording, and when participating in online lessons, all participants must work in an appropriate environment with a sensible background in school-appropriate attire.

16.4 Students and teachers should turn off or block cameras and microphones when class is not in session, and be sure that no personal information is in camera view.

16.5 Online lessons and student-teacher online conferences may only be recorded for safeguarding purposes by ACS staff. Digital files will be deleted according to the Data Retention Policy.

17.**Training**

17.1 All staff in a teaching and/or administrative role are required to be trained in online safety. ACS commits to ensuring online safety training remains up to date and is informed by current best practice. Online safety training is provided for Trustees, IT staff, School IT leaders, parents and students. All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

17.2 By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing and/or bullying messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, especially degrading images and depictions of violence against women
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff develop:

- better awareness to assist in spotting the signs and symptoms of online abuse
- the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- strategies to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

17.3 DSLs and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. DSLs, deputies and Online Safety Leads will also update their knowledge and skills about online safety at regular intervals, and at least annually.

18. Monitoring arrangements

Appointed school leaders log behaviour related to online safety in the Student Information System. DSLs document safeguarding issues related to online safety in MyConcern.

This policy will be reviewed every year by the Group DSL. At every review, the policy will be shared with the Heads of School and Board Education Sub-committee. The review will be supported by an annual risk assessment that considers and reflects the risks students and staff face online.

19. Associated policies

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

Acceptable Use Policy
Anti-bullying Policy
Behaviour Policy

Child on Child Abuse Prevention and Response Policy
Child Protection and Safeguarding Policy
Data Protection and Retention Policies
Exclusion Policy
Health and Safety Policy
Managing Allegations (including Low Level Concerns)
PSHE Policy
Privacy Notice
Relationships (and Sex) Education Policy
Staff Code of Conduct
Staff Disciplinary Procedure
Staff Social Media Guidelines
Student Mental Health Policy
Whistleblowing Policy

Appendices

Group Online Safety Lead Key Responsibilities

Online Safety Training Matrix

School Online Safety Advisory Group Terms of Reference

Resources and Key References for Guidance

Digital literacies curriculum standards

Digital Flourishing Model

Parent Education

Staff Resources

Group Online Safety Lead

OVERALL JOB PURPOSE

The Online Safety Lead oversees and manages the implementation and maintenance of internet filtering and monitoring systems within ACS. This role involves ensuring compliance with relevant policies and regulations, maintaining a safe online learning environment, and providing technical support to faculty, staff, and students. In collaboration with school-based technology leaders, this role oversees the development, implementation, and evaluation of K – 12 Online Learning Curriculum.

Key collaborators

- Group DSL, school DSLs and DDSLs
- Heads of School
- Head of IT, and key IT infrastructure and operation staff
- School-based technology leaders
- Senior Leader for Professional Learning and Growth
- External providers of Internet Filtering and Monitoring solutions

PRINCIPAL ACCOUNTABILITIES

Configure and maintain internet filtering and monitoring solutions on ACS student networks

- Configure content filtering rules and categories based on determined ACS Risk Profile, educational needs, and regulatory requirements
- Review and update filtering rules regularly to adapt to changing online threats and trends
- Establish protocols for handling incidents related to inappropriate content or online behaviour
- Generate regular reports on system performance, user activity, and incident trends
- Troubleshoot and resolve technical issues related to internet filtering and monitoring systems.
- Collaborate with IT support teams to address any hardware or software issues.
- Prioritise and lead on investigating high concern reports with the DSL team

Ensure compliance with local and national regulations regarding online content and user safety under the DfE Filtering and Monitoring Standards and KCSIE.

- Contribute relevant updates and assistance to the DSLs to support the completion of the Annual Prevent Risk Assessment
- Contribute to management and Board level reporting about online safety
- Contribute to the development and review of online safety policies
- Complete an annual Filtering and Monitoring Standards Audit with the Head of IT, Director of Education and Group DSL

Lead the development of an effective online safety curriculum

- Develop and provide a K - 12 Online Learning Curriculum which complies with the Education for a Connected World framework
- Provide training and support to Boarding students and faculty
- Support staff in their online safeguarding responsibilities through professional development and information campaigns

Continual Improvement

- Stay updated on emerging trends, technologies, and best practices in internet filtering and monitoring.
- Implement improvements to enhance the effectiveness of the filtering and monitoring systems.
- Maintain appropriate levels of training (CEOP Ambassador) and professional networking relationships

Online Safety Training Matrix

	Leading Online safety	Online Safety- SC	Online Safety Policy	High level training	Basic training
Trustees and Senior Leaders	Online Safety Questions for School Governors		X		NOS (optional for most Trustees)
School Leaders (MHS team)			X	INEQE Staying Safer Online (Intermediate or Advanced)	
Online Safety Leads and DSLs			X	DSL Safeguarding Training	CEOP KCSO NOS
IT professionals			X		
Counsellors, RSE Teachers, Year Group Leaders, SEN leads		X (3 years)	X		CEOP KCSO (optional)
SEN Leaders			X		NOS
Teachers and Other Professional Staff*		Grades 9-12 Grades 5-8 Grades 4 and below Multiple	X		

***Special Education Case Managers**

Children with SEND (Special Educational Needs and Disabilities) are more likely than their peers to experience online issues such as cyberbullying, online grooming and exploitation. Similarly, children with SEND are more likely to have their internet use restricted and therefore have limited opportunities to learn through experience, develop resilience or seek support, which would empower them to use technology safely.

School Online Safety Advisory Groups

Terms of Reference

Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy, including the impact of initiatives.

Membership

The Online Safety Advisory Groups will seek to include representation from all stakeholders.

The composition of the group should include:

1. Group Online Safety Leader
2. SLT member
3. Designated Safeguarding Lead
4. Teaching staff member
5. Support staff member
6. Online Safety Coordinator (not ICT coordinator by default)
7. Trustee
8. Parent/Carer
9. ICT Technical Support staff
10. Community users
11. Student representation for advice and feedback. Student voice is essential in the make-up of the online safety group, but students would only be expected to take part in committee meetings where deemed relevant.

Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

Functions of the Committee

The Committee assists the Online Safety Coordinator with the following:

1. To keep up to date with new developments in the area of online safety.

2. To review progress toward 360 Degrees Safe goals
3. To (at least) annually review and develop the Online Safety Policy in line with new technologies and incidents.
4. To monitor the delivery and impact of the Online Safety Policy.
5. To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching, learning and training.
6. To ensure that monitoring is carried out of Internet sites used across the school.
7. To monitor changes to filtering (e.g. requests for blocking and unblocking of sites).
8. To promote the safe use of data across the school, i.e. trends and cyber-security, GDPR, pupil data.
9. To monitor incidents involving cyberbullying for staff and pupils.
10. To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and developments in the area of online safety. This can be carried out through:
    - Staff meetings
    - Student forums (for advice and feedback)
    - Trustee meetings
    - Surveys for students, parents/carers and staff
    - Parents' evenings
    - Newsletters and the Learning Management System
    - Online safety events
    - Internet Safety Day (annually held on the second Tuesday in February).

Online Safety Group
(ACS Wide)

1. **Director of Education and Integrated Technology**
2. **Head of IT**
3. **Group DSL**
4. **Group Online Safety Leader**
5. **Data Protection Officer**
6. **Trustee/ Online Safety Champion**
7. **Online Safety Lead from each school**
8. **PSO representative (rotates)**
9. **School government representative (rotates)**

Resources and key references for guidance

Child Safety Online: a practical guide for providers of social media and interactive services (2016) (UK Council for Child Internet Safety);
(2023)
Safeguarding and remote education (2021)
Harmful online challenges and online hoaxes (2021)
Digital resilience framework (2020)
Sharing nudes and semi-nudes: advice for education settings working with children and young people (2024)
Education for a Connected World
Mobile phones in schools: Guidance for schools for prohibiting mobile phone use throughout the school day

Other trusted organisation whose work informs this policy include:

- UK Council for Internet Safety (UKCIS) guidance: Education for a connected world
- UK Safer Internet Centre guidance: Appropriate monitoring
- National Crime Agency's Child Exploitation and Online Protection Centre CEOP) education programme: Thinkuknow
- NSPCC
- SWGfL
- Surrey and Hillingdon Children's Safeguarding Partnerships
- Digital Resilience Working Group
- Educate Against Hate

Digital literacies curriculum standards

UK National standards for essential digital skills

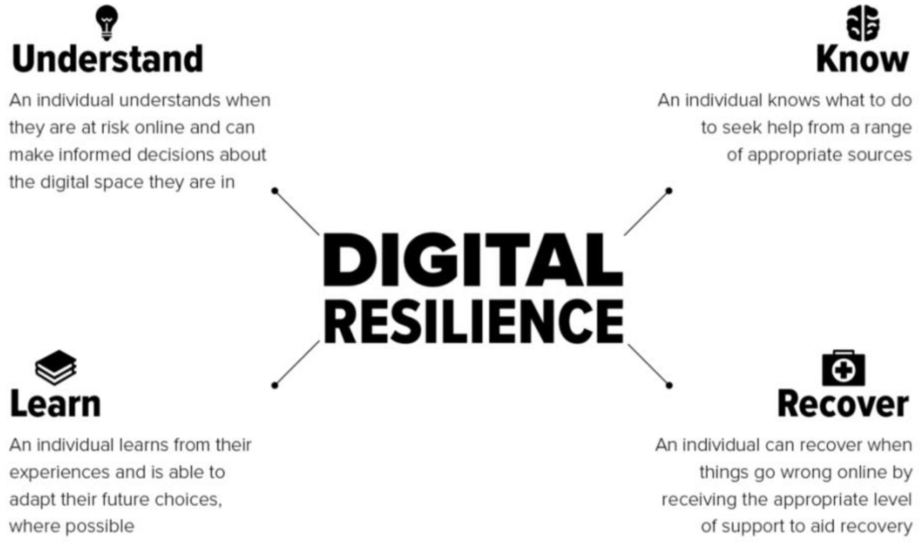
ISTE Standards for Students: Digital citizen

Students recognize the rights, responsibilities and opportunities of living, learning and working in an interconnected digital world, and they act and model in ways that are safe, legal and ethical.

- Students cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world.
- Students engage in positive, safe, legal and ethical behavior when using technology, including social interactions online or when using networked devices.
- Students demonstrate an understanding of and respect for the rights and obligations of using and sharing intellectual property.
- Students manage their personal data to maintain digital privacy and security and are aware of data-collection technology used to track their navigation online.

Digital Flourishing Model

Digital resilience framework



DIGITAL RESILIENCE

Understand

An individual understands when they are at risk online and can make informed decisions about the digital space they are in

Know

An individual knows what to do to seek help from a range of appropriate sources

Learn

An individual learns from their experiences and is able to adapt their future choices, where possible

Recover

An individual can recover when things go wrong online by receiving the appropriate level of support to aid recovery

Parent education

Topics to discuss with students

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

The Key Parent Information Guides

Online safety organisations

- The National College (Online Safety)
- Connect Safely
- Family Online Safety Institute (Good Digital Parenting)
- Be Internet Awesome (In collaboration with Google)
- Net-aware has support for parents and carers from the NSPCC, including a guide to social networks, apps and games
- Keeping children and young people safe from radicalisation
- Advice for parents on keeping children safe online (UK Government)

- UK Safer Internet Centre has tips, advice, guides and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services
- Internet Matters (in collaboration with Sky) has advice for parents of students with special education needs and disabilities
- Harmful online challenges and online hoaxes
- Ineqo Safety Centre
- The National College (Online Safety)

The Internet Watch Foundation and NSPCC provide facilitities to report (and remove) online child sexual abuse and nude images shared online.

Mobile devices/ parental controls

Ofcom: Parents' controls for mobile phones
Vodafone: Staying in Touch: A Parent's Guide to Mobile Phones
BT: Parental controls guide
ATT: Family Media Plan

Staff Resources

Teacher Checklist (Childnet International)

ISTE Standards for Educators: Digital citizenship

Educators inspire students to positively contribute to and responsibly participate in the digital world. Educators:

- create experiences for learners to make positive, socially responsible contributions and exhibit empathetic behavior online that build relationships and community.
- establish a learning culture that promotes curiosity and critical examination of online resources and fosters digital literacy and media fluency.
- mentor students in safe, legal and ethical practices with digital tools and the protection of intellectual rights and property.
- model and promote management of personal data and digital identity and protect student data privacy.

https://projectevolve.co.uk/guidance/curriculum-planning/Project Evolve provides suggestions for integrating digital safety into subject-specific curriculum objectives.

The UK Safer Internet Centre provide information for staff about managing professional online reputations.

SWGfL provides an intimate abuse/ revenge porn helpline for adults, and a platform for reporting harmful online content, as well as information about AI and online safety.

Ineqe Safeguarding Group provide a Home Learning Hub with downloadable resources.

Report Remove Childline Reporting tool

TALK and Gurls Out Loud IWF Campaign