



ICT, INTERNET AND ACCEPTABLE USE POLICY

W04

Policy owner:	Heads of Digital Learning
---------------	---------------------------

Policy agreed on:	June 2022
-------------------	-----------

Policy reviewed on:	June 2026
---------------------	-----------

Policy to be reviewed on:	June 2027
---------------------------	-----------

DOCUMENT CONTROL TABLE

Status		Live
Policy owner		Head of Digital Learning
Statutory/Recommended		Recommended
Date approved		June 2022
Review period		1yr
Latest review date		June 2026
Next review date		June 2027
Linked documents and policies		Safeguarding & Child Protection Policy Data Protection Policy Social Media Policy Keeping Children Safe in Education
Version	Date	Comments
2	November 2023	Whole policy rewritten in line with KSCIE 2023 updates
2.1	September 2024	Policy updated with phone pouches
2.2	August 2025	Updated in line with changes from KCSIE 2025 Safeguard children from misinformation, disinformation, and conspiracy theories as identified in KCSIE 2025 Added in: Filtering and monitoring section Parents must consent for their child's photos to be taken at admission and for trips.
2.3	June 2026	Updated to incorporate proposed changes from the KCSIE 2026 Updates include: revised terminology for self-generated intimate images (including AI-generated deepfakes); new section on misogyny and harmful sexual behaviour online; expanded AI safeguarding section referencing DfE updated policy paper (2025/2026) and Chiltern Learning Trust/Chartered College of Teaching resources; filtering and monitoring updated to require annual documented review with records of checks across all internet-connected devices; cybersecurity explicitly elevated to a safeguarding concern; DSL cover arrangements and skills/experience requirement added; new references to CEOP/IWF AI-generated CSAM guidance and CEOP FMSE guidance for education settings; 'racism' and 'derogatory behaviour' added to curriculum and aims sections.

PURPOSE	4
AIMS	4
LEGISLATION AND GUIDANCE	5
FILTERING AND MONITORING	6
ROLES AND RESPONSIBILITIES	7
EDUCATING PARENTS ABOUT ONLINE SAFETY	13
CYBER-BULLYING	13
MISOGYNY AND HARMFUL SEXUAL BEHAVIOUR ONLINE	15
CYBERSECURITY AWARENESS	16
ARTIFICIAL INTELLIGENCE (AI)	17
ACCEPTABLE USE OF TECHNOLOGY IN SCHOOL	18
PUPILS USING MOBILE DEVICES IN SCHOOL	18
USER-CREATED CONTENT AND ISLAMIC VALUES	18
STAFF USING WORK DEVICES OUTSIDE SCHOOL	19
HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE	20
TRAINING	20
APPENDIX 1 - PUPIL ACCEPTABLE USE OF TECHNOLOGY – EXPECTATIONS	22
APPENDIX 2 - PUPIL ACCEPTABLE USE OF TECHNOLOGY – EXPECTATIONS: PRIMARY	23
APPENDIX 3: PUPIL ACCEPTABLE USE OF TECHNOLOGY – EXPECTATIONS: SECONDARY	25
APPENDIX 4 – ONLINE SAFETY TRAINING NEEDS: SELF-AUDIT FOR STAFF	27
APPENDIX 5 – ACCEPTABLE USE AGREEMENT FOR STAFF & GOVERNORS	28
APPENDIX 6 – ONLINE SAFETY INCIDENT LOG REPORT	29

PURPOSE

This policy is directly related to our school's vision, **Inspiring Minds** and is underpinned by our Core **Values of Discovery, Courage and Humanity**. It sets out the principles and expectations that govern the safe, responsible, and ethical use of technology across the Doha College community.

We believe that technology, when used well, is a powerful tool for learning and discovery. It enables pupils to explore new ideas, connect with the world around them, and develop the skills they need to thrive in an increasingly digital society. At the same time, we recognise that the online world presents real risks, and that it is our responsibility to equip every member of our community with the knowledge and confidence to navigate it safely.

Our approach to online safety reflects the qualities of our Learner Profile. We encourage pupils to be curious and open to new experiences, whilst also being courageous enough to make responsible choices, seek help when needed, and stand up for what is right. We expect all members of our community to act with kindness, honesty and empathy both online and offline and to treat others with respect, celebrating the diversity and individuality that makes our school community so strong.

This policy applies to all pupils, staff, governors, volunteers, and visitors.

AIMS

Doha College aims to:

- Have robust processes to ensure the online safety of pupils, staff, volunteers, and governors.
- Identify and support groups of pupils who may be at greater risk of harm online than others.
- Deliver a practical approach to online safety, which empowers us to protect and educate the whole school community in its use of mobile and smart technology (which we refer to as 'mobile devices').
- Establish precise mechanisms to identify, intervene in, and, where appropriate, escalate an incident.
- Safeguard children from misinformation, disinformation, and conspiracy theories as identified in KCSIE 2026.
- Maintain zero tolerance for misogyny, racism, and other derogatory behaviour, recognising the link between extreme misogyny and harmful sexual behaviour.

The four key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content: being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, antisemitism, self-harm, suicide, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual and non-consensual self-generated intimate images and/or videos including those generated using AI, e.g. deepfakes), sharing other explicit images and online bullying; and

Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2026, which Doha College adopts as a best-practice framework. Relevant DfE advice referenced includes:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

As a British curriculum school operating in Qatar, this policy is further informed by and must be read alongside the following Qatari legal and regulatory frameworks:

- **Qatar Law No. 13 of 2014 (Cybercrime Prevention Law)** — which criminalises unauthorised access to computer systems, the distribution of content that violates public order or Islamic values, and the creation or sharing of illegal online content.

- **Qatar Law No. 15 of 2014 (Child Protection Law)** — which establishes the rights of children to protection from all forms of harm, abuse, and exploitation, including through digital means.
- **Qatar Law No. 3 of 2016 (Personal Data Privacy Protection Law)** — which governs the collection, storage, and processing of personal data, including data relating to minors.
- **Qatar Ministry of Education and Higher Education (MoEHE) regulations** — which set out the standards and expectations for schools operating in Qatar, including British curriculum schools.
- **Qatar's Ministry of Education and Higher Education guidelines** on acceptable use of technology in educational settings.

Where Qatari law imposes stricter requirements than DfE guidance, Qatari law takes precedence. In particular, staff and pupils should be aware that the sharing or viewing of sexually explicit material, including pornography, is a criminal offence in Qatar carrying severe penalties. The creation or distribution of content that contravenes Islamic values or Qatari customs is also subject to legal sanction.

The policy also takes into account the National Curriculum computing programmes of study and the DfE's guidance on the use of reasonable force, adapted where necessary to reflect Qatari legal standards and school context.

FILTERING AND MONITORING

Doha College maintains robust filtering and monitoring provisions on all school devices and networks, including all internet-connected devices in all relevant locations. In line with KCSIE 2026, these provisions include:

- Daily alerts
- Immediate alerts for high-risk incidents
- User login notices reminding staff/pupils that devices are monitored
- All checks logged with date/time, staff member, and actions taken
- A formal documented review carried out at least once every academic year, including checks that filtering is working appropriately on all internet-connected devices in all relevant locations, with a record kept of all checks, in line with KCSIE 2026.
- Annual self-assessment using the DfE's Plan Technology for your School tool to assess effectiveness against the DfE Filtering and Monitoring Standards and receive personalised recommendations

- Compliance with the DfE Generative AI: product safety expectations, which clarify how filtering and monitoring requirements apply to the use of generative AI in education
- Annual review of filtering and monitoring provisions by the Governing Board

ROLES AND RESPONSIBILITIES

The Governing Board

The Governing Board monitors this policy and holds the executive designated safeguarding lead (EDSL) accountable for its implementation.

The Governing Board, alongside the Heads of Digital Learning and EDSL, will ensure all staff undergo online safety training as part of child protection and safeguarding training, and that staff understand their expectations, roles, and responsibilities regarding filtering and monitoring.

The Governing Board, EDSL, and Heads of Digital Learning will also ensure that all staff receive regular online safety updates (via email, newsletters, and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to safeguard children effectively.

The Governing Board will coordinate regular meetings with appropriate staff to discuss online safety training requirements and monitor online safety logs as provided by EDSL. The Governing Board should ensure that children are taught how to keep themselves and others safe, including online safety.

The Governing Board must ensure the school has appropriate filtering and monitoring systems on school devices and networks and will regularly review their effectiveness, carrying out a formal, documented review at least once every academic year. 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 those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Carrying out a documented review of filtering and monitoring provisions at least once every academic year, including checks on all internet-connected devices in all relevant locations, with records kept.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.

- Have effective monitoring strategies to meet their safeguarding needs, by ensuring annual self-assessment using the DfE's Plan Technology for your School tool.

All governors will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 5).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND).

The EDSL/DSLs

The EDSL/DSLs take the lead responsibility for online safety in school. In line with KCSIE 2026, the EDSL must hold appropriate status, authority, and the practical skills and experience needed to carry out its responsibilities effectively. Robust cover arrangements must be in place to ensure safeguarding concerns are addressed without delay when the EDSL is unavailable.

Responsibilities include:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Principal and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the Head of IT to make sure the appropriate systems and processes are in place.
- Working with the Principal, Head of IT and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's safeguarding policy.
- Ensuring that any online safety incidents are logged on CPOMS and handled appropriately in line with this policy.
- Ensuring that any incidents of cyberbullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy.

- Updating and delivering staff training on online safety (Appendix 4 contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Principal and/or governing board.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually.

This list is not intended to be exhaustive

The Head of IT

The Head of IT is responsible for:

- Putting in place an appropriate level of security protection, such as content filtering, device management and firewalls which filter content and protect the perimeter network. These are reviewed and updated at least annually to assess their effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monthly monitoring of the school's ICT systems.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged via CPOMS (see Appendix 6) and dealt with appropriately in line with this policy.
- Ensuring that cyber-bullying incidents are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

The Head of Digital Learning (Primary and Secondary)

The HODLs are responsible for:

- Supporting the IT team in monitoring the appropriate level of security protection, such as filtering and monitoring systems on school devices (Jamf) and school networks.
- Ensuring the school's ICT systems are regularly communicated to all stakeholders.
- Conducting frequent pupil checks for any security risks and threats.
- Monitoring the signing of staff and pupils' Acceptable Use contracts.
- Delivering training to both pupils and staff about acceptable use and online safeguarding.

- Checking and tracking appropriate applications and software for school use.

This list is not intended to be exhaustive.

All Staff and Volunteers

- All staff, including contractors, agency staff, and volunteers, are responsible for:
- Maintaining an understanding of this policy.
- Implement this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 5), and ensuring that pupils follow the school's terms on acceptable use (Appendices 1, 2, and 3).
- Knowing that the EDSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting the Helpdesk email.
- Following the correct procedures by contacting the Helpdesk email if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the EDSL to ensure that any online safety incidents are logged (see Appendix 6) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify the Head of Digital Learning, EDSL, or the Principal of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International

- Parent resource sheet – Childnet International

Visitors and Members of the Community

Visitors and community members who use the school's ICT systems or the internet will be made aware of this policy when relevant and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 5).

Educating Pupils About Online Safety

It is essential that pupils are safeguarded from potentially harmful and inappropriate online material. An effective whole-school approach to online safety empowers us to protect and educate pupils on their use of technology, and to establish mechanisms to identify, intervene in, and escalate concerns where appropriate.

Pupils will be taught about online safety, digital footprint, digital citizenship, and well-being as part of the curriculum:

- In Computer Science lessons.
- In PSHCE lessons.
- In Media at KS4/5.
- In Digital induction, assemblies, and Internet Safety Week.
- As part of Media Literacy Week.
- Through work done by the pupil Digital Committee.

In EYFS, KS1, KS2, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact, and conduct, and know how to report concerns.
- Understand the impact of their digital footprint and the harmful effects of overusing technology.

Pupils in KS3, KS4, and Key Stage 5 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- Recognise inappropriate content, contact, and conduct, and know how to report concerns.
- Understand the impact of their digital footprint.

- Awareness of social and psychological issues related to electronic device usage, including the benefits and challenges of social media use.
- The importance of using technology and AI responsibly and ethically, using critical thinking skills to question and validate material, including identifying misinformation, disinformation, and conspiracy theories.
- The harms of misogyny and how extreme misogynistic ideologies online can contribute to the normalisation of sexual harassment and harmful sexual behaviour, in line with KCSIE 2026 proposals.
- Awareness of sextortion and financially motivated sexual extortion (FMSE), including the risks posed by gaming platforms and social media as sites where grooming, exploitation, and coercion can occur.

By the end of secondary school, pupils will know:

- Their rights, responsibilities, and opportunities online, including that the same behaviour expectations apply in all contexts, including online.
- Online risks, including any material someone provides to another that has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want to be shared further and not to share personal material sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- Sharing and viewing sexually explicit material (e.g., pornography) is a criminal offence in Qatar that carries severe penalties, including jail.
- That sharing and viewing indecent images of children (including those created by children, or generated using AI) is a criminal offence that carries severe penalties, including jail.
- How information and data are generated, collected, shared, and used online.
- How to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report or find support if they have been affected by those behaviours.

Key external resources referenced in KCSIE 2026:

DfE advice for schools: teaching online safety in schools

- UK Council for Internet Safety (UKCIS) guidance: Education for a connected world
- UKCIS external visitors guidance

- National Crime Agency's CEOP Education Programme: Protecting children and young people from online child sexual abuse through education
- CEOP Education / Internet Watch Foundation: Understanding and responding to AI-generated child sexual abuse material (KCSIE 2026 proposal)
- CEOP Education: Financially Motivated Sexual Extortion (FMSE) – guidance for education settings (KCSIE 2026 proposal)
- UK Health Security Agency: Every Mind Matters
- Harmful online challenges and online hoaxes guidance

EDUCATING PARENTS ABOUT ONLINE SAFETY

The school will raise parents' awareness of internet safety through letters and other home communications, as well as information on our website or Google Site. They will all be given access to The National Online Safety via logins and educated about this in parent presentations. This policy will also be shared with parents/carers.

The school will let parents know:

- What systems does the school use to filter and monitor online use?
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.
- Parents must consent to photographs at admission; check consent before trips and events.

If parents have any queries or concerns about online safety, these should be raised with the Principal or EDSL in the first instance. Concerns or queries about this policy can be raised with any member of staff, but the Heads of Digital Learning or EDSL would be best placed to address them.

CYBER-BULLYING

Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. Preventing and addressing cyberbullying

To help prevent cyberbullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how to

report incidents and are encouraged to do so, including when they are witnesses rather than the victim.

The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors and class teachers will discuss cyberbullying with their groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education and other subjects where appropriate.

All staff, governors, and volunteers receive training on cyberbullying, its impact, and ways to support pupils as part of safeguarding training.

The school also sends information on cyberbullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In the event of a specific incident of cyberbullying, the school will follow the procedures outlined in the School Behaviour Policy.

The EDSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if deemed necessary.

Examining electronic devices

The Principal/EDSL, and any member of staff authorised to do so by the Principal, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence about an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff.
- Explain to the pupils why they are being searched and how the search will happen.
- Seek the pupil's co-operation.

Authorised staff members may examine and, in exceptional circumstances, erase any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

If a staff member suspects a device may contain an indecent image of a child (also known as a consensual or non-consensual self-generated intimate image, including AI-generated images or deepfakes), they will:

- Not view the image.
- Confiscate the device and report the incident to the EDSL immediately, who will decide what to do next in line with the DfE's latest guidance on screening, searching and confiscation and UKCIS guidance.

Any searching of pupils will be carried out in line with the DfE's latest guidance on searching, screening, and confiscation, UKCIS guidance, our behaviour policy, and Qatar laws. Any complaints will be dealt with through the school's complaints procedure.

MISOGYNY AND HARMFUL SEXUAL BEHAVIOUR ONLINE

In line with KCSIE 2026, Doha College explicitly recognises misogyny as a safeguarding risk, particularly in the online context. Extreme misogyny is increasingly prevalent online and is often linked to harmful sexual behaviour (HSB) among young people.

Misogynistic ideologies can contribute to:

- The normalisation of sexual harassment and sexual violence.
- Child-on-child exploitation and coercion.
- The spread of harmful narratives, including through social media, gaming platforms, and other online spaces.

The school addresses online misogyny through:

- Curriculum content in PSHE, RSHE, and assemblies explicitly naming and countering misogynistic content.
- Zero tolerance for misogynistic language or behaviour, both online and offline, in line with the school behaviour policy.
- Staff training to recognise how exposure to misogynistic content online may manifest in pupil attitudes and behaviour.
- Signpost pupils and parents/carers to appropriate support where harmful attitudes are identified.

Staff should also be alert to the growing risk of sextortion, particularly financially motivated sexual extortion (FMSE), which can disproportionately affect young males. Offenders often coerce victims on gaming platforms, social media, or dating apps into sharing intimate images and then demand money under threat of exposure. Any suspected incident of FMSE should be referred immediately to the EDSL and, where appropriate, to the police.

CYBERSECURITY AWARENESS

All pupils and staff must complete mandatory cybersecurity awareness training to understand the risks of cybercrime and learn best practices for online safety.

Cybersecurity is now recognised as a safeguarding concern, not merely an IT concern. Schools hold sensitive personal data about children, including safeguarding records and health information. If this data is compromised through a cyber-attack, this can pose immediate risks to a child's safety and wellbeing. Doha College takes appropriate action to work towards the Cyber Security Standards for Schools and Colleges, developed to help schools improve their resilience against cyber-attacks. Broader guidance is available at the National Cyber Security Centre (NCSC).

Data Protection:

The school emphasises the importance of safeguarding sensitive data. All members of the school community are required to follow data protection protocols, including secure storage, encryption, and regular data backups.

Prohibited Activities:

Engaging in any form of cybercrime, including hacking, unauthorised access, malware distribution, phishing, or any illegal online activity, is strictly prohibited on the school's network.

Reporting Incidents:

Individuals who suspect or witness any cybercrime-related activity must promptly report it to the EDSL/DSLs. Where a child shows particular skills and interest in computing and technology and may be at risk of straying into cyber-dependent crime, the EDSL should consider a referral to the national Cyber Choices programme.

Consequences and Legal Compliance:

Violation of this policy may result in disciplinary actions, which could include suspension or expulsion for pupils and termination for staff. In some circumstances, the police will need to be notified. The IT team will fully cooperate with law enforcement authorities in the investigation and prosecution of cybercrime offences.

ARTIFICIAL INTELLIGENCE (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils, and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Doha College recognises that AI has many uses to help pupils learn but may also present risks, including misinformation, disinformation, the creation of 'deep fakes', and significant safeguarding harms.

Any misuse of AI to bully or harm others will be addressed under both the Behaviour Policy and the Safeguarding and Child Protection Policy.

This section is informed by the DfE's updated policy paper on the use of generative artificial intelligence in education (2025/2026), as referenced in KCSIE 2025 and the KCSIE 2026 consultation. The DfE policy paper outlines key safety considerations and legal responsibilities for schools when using generative AI in both teacher-facing and pupil-facing contexts.

[AI Companion Guide Link](#)

Key AI safeguarding considerations for Doha College:

- Staff must carry out a risk assessment before adopting any new AI tool in school, ensuring it meets the DfE's Generative AI: product safety expectations.
- AI-related risks are included in our Filtering and Monitoring framework, which is reviewed at least annually.
- Filtering and monitoring provisions must cover generative AI tools in line with DfE guidance.
- The creation, storage, or sharing of AI-generated intimate images (deepfakes) involving children is a criminal offence and will be treated as a serious safeguarding matter.
- Pupils are educated about the responsible and ethical use of AI, including the risks of misinformation, data privacy, and deepfake content, through assemblies, tutor lessons, and the Doha College AI Acceptable Use Companion Guide.
- All parents, pupils and the wider community will be provided with clear guidance about the ethical and effective use of AI through our Artificial Intelligence Companion Guide.

ACCEPTABLE USE OF TECHNOLOGY IN SCHOOL

All pupils, parents, staff, volunteers, and governors are required to sign an agreement regarding the acceptable use of the school's ICT systems and the Internet (Appendices 1 to 3).

Use of the school's internet must be for educational purposes only or to fulfil the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors, and visitors via firewall and content filtering systems to ensure compliance with the above and, where appropriate, restrict access through filtering systems.

- Staff must not take or store images or recordings of pupils on personal devices.
- Only school equipment may be used for pupil images or video.
- Staff must follow search and confiscation procedures where safeguarding concerns exist.
- Staff must not use personal phones in teaching areas, playgrounds, or wherever children are present, except in an emergency.

PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils may bring mobile devices to school but are not permitted to use them while on campus. Mobile phones must be placed in the phone pouches (YondR system). Any use of mobile devices by pupils at school must be in line with the acceptable use agreement. Any breach may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

USER-CREATED CONTENT AND ISLAMIC VALUES

The school will not take responsibility for content created by staff or pupils.

Respect for Diversity:

All user-created content within the school network must adhere to the principles of respect and inclusivity, ensuring that Islamic values are respected at all times.

Avoiding Offensive Material:

Users are prohibited from creating or sharing content that may be offensive or disrespectful towards Islamic values and Qatari customs and traditions.

Cultural Sensitivity:

Users are encouraged to be culturally sensitive when creating or sharing content.

Moderation and Reporting:

Users are encouraged to report any content that they believe violates these guidelines.

Educational Resources:

Training is given during the induction process regarding educational resources. The Resource Review Committee can advise on which materials can be used - rrccommittee@dohacollege.com

STAFF USING WORK DEVICES OUTSIDE SCHOOL

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keep the device password-protected and use strong passwords of at least 14 characters, combining uppercase and lowercase letters, numbers, and special characters.
- Not allowing their own children access to school devices/passwords.
- Using multi-factor authentication software for confidential information, such as emails/ISAMs.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Allowing anti-virus and anti-spyware software to automatically update.
- Keeping operating systems up to date by always allowing automatic updates.

Staff members must not use the device in any way that would violate the school's terms of acceptable use. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the IT manager or EDSL.

- Staff must not use personal phones during contact time with pupils, unless in an emergency.
- Staff must not take or store images or recordings of pupils on personal devices.
- Only school equipment may be used for pupil images or video.
- Personal phones should be used only in non-contact time and never in the presence of children.

HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour, ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device, where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. We will consider whether incidents involving illegal activity or content, or other serious incidents, should be reported to the police.

TRAINING

All new staff members will receive training and logins to access online courses from National Online Safety as part of their induction, on safe internet use and online safeguarding issues, including cyberbullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, along with relevant updates as required.

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

- Technology is a significant component in many safeguarding and wellbeing issues, and children are at risk of online abuse.

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of self-generated intimate images and/or videos (including AI-generated content), especially around chat groups
- Sharing of abusive images and pornography to those who do not want to receive such content
- Sextortion and financially motivated sexual extortion (FMSE), particularly targeting young males via gaming platforms, social media, and dating apps
- Physical abuse, sexual violence, and initiation/hazing-type violence can all contain an online element.
- Extreme misogyny online can contribute to harmful sexual behaviour and the normalisation of sexual harassment.

Training will also help staff:

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

The EDSL/DSLs and deputies will undertake child protection and safeguarding training, including online safety, at least every 2 years. They will also update their knowledge and skills on online safety at regular intervals, at least annually. Governors will receive training on safe internet use and online safeguarding as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

APPENDIX 1 - PUPIL ACCEPTABLE USE OF TECHNOLOGY – EXPECTATIONS

As a pupil, you are expected to use technology safely and responsibly. Please read the information below to acknowledge you have understood this.

All pupils will

Ensure their devices are brought to school everyday fully charged, installed with Jamf (if using an iPad) and all software is kept up to date.

Ensure they bring suitable headphones to school everyday.

KSS and those with a laptop provision - Ensure their M.A.C address is registered with the IT department.

Keep their usernames and passwords private.

Take personal responsibility for any additional hardware such as Apple pencils, covers, screen protectors.

Treat others with respect and use appropriate language in all of my electronic interactions with others.

Immediately tell a teacher or other adult staff member if they receive an electronic comment or communication that makes me feel uncomfortable, or if they accidentally access inappropriate materials, pictures, video, or websites.

Respect the work and intellectual property rights of others, and they will not intentionally copy, damage, or delete another user's work.

Respect the privacy of others. They will limit all in-school photography, video and audio recording to educational use.

Comply with the YondR mobile phone policy: either leave mobile at home or store in a YondR Pouch.

Follow the Doha College AI Acceptable Use guide.

All pupils will not:

Use devices that are not connected to Jamf or registered with IT.

Use their mobile phone while on campus - any visible phone will be confiscated if not in YondR pouch.

Use their iPad, laptop or headphones without permission from the teacher first.

Use technology in school or out, to find, create, or send information to spread lies or misinformation; or harass, harm, or bully others.

Use technology to gain unauthorised or inappropriate access to school or pupil resources.

Use, retrieve, store, or send improper or culturally insensitive language, pictures, or other digital content.

Use technology or their personal electronic device to cheat or plagiarise - for example: they will not get or give answers to tests; search for and / or copy answers or information on the internet or other electronic resources contained on or in any technology resource or device; copy and submit someone else's information or assignment as my own; or conduct other similar forms of electronic cheating using AI.

Access inappropriate or blocked resources using personal Wi-Fi accounts, 3G/4G/5G VPNs, or by any other manner during school hours.

Share or post any personally identifiable information about others or themselves that could help someone locate or contact others or them. This includes such things as e-mail address, full name, home or school address, phone number, parent's or guardian's names, and school name.

All pupils understand:

Use of technology resources, including networks, computers or mobile devices, and the Internet is a privilege, which may be denied, revoked, or restricted at any time for misuse or abusive conduct.

Doha College reserves all rights to control its technology resources and may monitor or restrict a user's technology resources.

Online learning spaces and communication and collaboration tools should be treated as a classroom space, and language and behavior that is not appropriate in the physical classroom is not appropriate in online spaces, no matter what time of day those spaces are accessed.

Assignments in online learning spaces are just like any other assignment in school, and pupils are expected to demonstrate integrity with relation to cheating, plagiarism, and acceptable use of technology.

Personal electronic devices are at an increased risk of being stolen, misplaced, or damaged, and Doha College is not responsible for any loss, damage or theft of personal property.

Pupils may be subject to disciplinary action for using technology in violation of Doha College's policies, procedures, guidelines

APPENDIX 2 - PUPIL ACCEPTABLE USE OF TECHNOLOGY – EXPECTATIONS: PRIMARY

As a pupil, you are expected to use technology safely and responsibly. Please read the information below to acknowledge you have understood this.

All pupils will:

In FS1-Y2: Ensure they use all school technology with care and in the presence of an adult.

In Y3-6: Ensure their devices are brought to school every day fully charged, installed with Jamf (if using an iPad) and all software is kept up to date.

In Y3-6 Ensure they bring suitable headphones to school every day.

Keep their usernames and passwords private.

Take personal responsibility for any additional hardware such as Apple pencils, covers, screen protectors.

Treat others with respect and use appropriate language in all of my electronic interactions with others.

Immediately tell a teacher or other adult staff member if they receive an electronic comment or communication that makes me feel uncomfortable, or if they accidentally access inappropriate materials, pictures, video, or websites.

Comply with the YondR mobile phone policy: either leave mobile at home or store in a YondR Pouch.

Respect the work and intellectual property rights of others, and they will not intentionally copy, damage, or delete another user's work.

Respect the privacy of others. They will limit all in-school photography, video, and audio recording to educational use.

All pupils will not:

Use devices that are not connected to Jamf or registered with IT.

Use their mobile phone while on campus

Use their iPad, laptop, or headphones without permission from the teacher first.

Use technology in school or out, to find, create, or send information to spread lies or misinformation; or harass, harm, or bully others.

Use technology to gain unauthorised or inappropriate access to school or pupil resources.

Use, retrieve, store, or send improper or culturally insensitive language, pictures, or other digital content.

Use technology or their personal electronic device to cheat or plagiarise - for example: they will not get or give answers to tests; search for and / or copy answers or information on the internet or other electronic resources contained on or in any technology resource or device; copy and submit someone else's information or assignment as my own; or conduct other similar forms of electronic cheating using AI.

Access inappropriate or blocked resources using personal Wi-Fi accounts, 3G/4G/5G VPNs, or by any other manner during school hours.

Share or post any personally identifiable information about others or themselves that could help someone locate or contact others or them. This includes such things as e-mail address, full name, home or school address, phone number, parent's or guardian's names, and school name.

Create or share material that is culturally inappropriate, in keeping with Qatari and Islamic values.

All pupils understand:

Use of technology resources, including networks, computers or mobile devices, and the Internet is a privilege, which may be denied, revoked, or restricted at any time for misuse or abusive conduct.

Doha College reserves all rights to control its technology resources and may monitor or restrict a user's technology resources.

Online learning spaces and communication and collaboration tools should be treated as a classroom space, and language and behaviour that is not appropriate in the physical classroom is not appropriate in online spaces, no matter what time of day those spaces are accessed.

Assignments in online learning spaces are just like any other assignment in school, and pupils are expected to demonstrate integrity with relation to cheating, plagiarism, and acceptable use of technology.

Personal electronic devices are at an increased risk of being stolen, misplaced, or damaged, and Doha College is not responsible for any loss, damage, or theft of personal property.

Pupils may be subject to disciplinary action for using technology in violation of Doha College's policies, procedures, guidelines.

APPENDIX 3: PUPIL ACCEPTABLE USE OF TECHNOLOGY – EXPECTATIONS: SECONDARY

As a pupil, you are expected to use technology safely and responsibly. Please read the information below to acknowledge you have understood this.

All pupils will:

Ensure their devices are brought to school everyday fully charged, installed with Jamf (if using an iPad) and all software is kept up to date.

Ensure they bring suitable headphones to school every day.

KS5 - Ensure their M.A.C address is registered with the IT department.

Keep their usernames and passwords private.

Take personal responsibility for any additional hardware such as Apple pencils, covers, screen protectors.

Treat others with respect and use appropriate language in all of my electronic interactions with others.

Immediately tell a teacher or other adult staff member if they receive an electronic comment or communication that makes me feel uncomfortable, or if they accidentally access inappropriate materials, pictures, video, or websites.

Comply with the YondR mobile phone policy: either leave mobile at home or store in a YondR Pouch.

Respect the work and intellectual property rights of others, and they will not intentionally copy, damage, or delete another user's work.

Respect the privacy of others. They will limit all in-school photography, video, and audio recording to educational use.

All pupils will not:

Use devices that are not connected to Jamf or registered with IT.

Use their mobile phone while on campus

Use their iPad, laptop, or headphones without permission from the teacher first.

Use technology in school or out, to find, create, or send information to spread lies or misinformation; or harass, harm, or bully others.

Use technology to gain unauthorised or inappropriate access to school or pupil resources.

Use, retrieve, store, or send improper or culturally insensitive language, pictures, or other digital content.

Use technology or their personal electronic device to cheat or plagiarise - for example: they will not get or give answers to tests; search for and / or copy answers or information on the internet or other electronic resources contained on or in any technology resource or device; copy and submit someone else's information or assignment as my own; or conduct other similar forms of electronic cheating using AI.

Access inappropriate or blocked resources using personal Wi-Fi accounts, 3G/4G/5G VPNs, or by any other manner during school hours.

Share or post any personally identifiable information about others or themselves that could help someone locate or contact others or them. This includes such things as e-mail address, full name, home or school address, phone number, parent's or guardian's names, and school name.

All pupils understand:

Use of technology resources, including networks, computers or mobile devices, and the Internet is a privilege, which may be denied, revoked, or restricted at any time for misuse or abusive conduct.

Doha College reserves all rights to control its technology resources and may monitor or restrict a user's technology resources.

Online learning spaces and communication and collaboration tools should be treated as a classroom space, and language and behavior that is not appropriate in the physical classroom is not appropriate in online spaces, no matter what time of day those spaces are accessed.

Assignments in online learning spaces are just like any other assignment in school, and pupils are expected to demonstrate integrity with relation to cheating, plagiarism, and acceptable use of technology.

Personal electronic devices are at an increased risk of being stolen, misplaced, or damaged, and Doha College is not responsible for any loss, damage, or theft of personal property.

pupils may be subject to disciplinary action for using technology in violation of Doha College's policies, procedures, guidelines.

APPENDIX 4 – ONLINE SAFETY TRAINING NEEDS: SELF-AUDIT FOR STAFF

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors, and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	

ONLINE SAFETY TRAINING NEEDS AUDIT

Are there any areas of online safety in which you would like training/further training?

APPENDIX 5 – ACCEPTABLE USE AGREEMENT FOR STAFF & GOVERNORS

Acceptable use of the school's ICT facilities and the internet: agreement for staff and governors

Name of staff member/governor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to or send such material)

Use them in any way which could harm the school's reputation.

Access social networking sites or chat rooms

Use any improper language when communicating online, including in emails or other messaging services.

Install any unauthorised software or connect unauthorised hardware or devices to the school's network.

Share my password with others or log in to the school's network using someone else's details.

Share confidential information about the school, its pupils or staff, or other members of the community.

Access, modify or share data I'm not authorised to access, modify or share.

Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) know if a pupil informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governor):

Date:

--	--

APPENDIX 6 – ONLINE SAFETY INCIDENT LOG REPORT

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

