

Online Safety Policy 2026-2028

Last reviewed on: June 2026

Next review due by: June 2028

Table of Contents

Purpose.....	3
Scope	3
Legislation and Guidance	3
Types of Risks.....	3
Inappropriate Content.....	4
Roles & Responsibilities.....	4
School Board	4
Regional Head of Schools (RHoS)	4
Principal and senior leaders.....	4
DECE/Designated Safeguarding Lead (or Deputy)	5
Network/IT Manager and technical staff	5
Teaching and Support Staff	6
Students.....	6
Parents	6
Visitors and members of the community.....	6
Education and Training	6
Students' Education	7
Primary School	7
Secondary school	8
Parent Education and Engagement	8
Staff/Volunteers Education and Engagement	9
Regional Head of Schools (RHoS) and School Board	9
Dealing With Incidents of Misuse.....	9
Incidents.....	9
Mandatory Police Referral	9
Safeguarding Measures.....	10
Actions and Sanctions	10
Cyber-bullying.....	10
Definition	10
Preventing and Addressing Cyber-Bullying	10
Examining Electronic Devices.....	11
Artificial Intelligence (AI).....	12
Acceptable Use of the Internet in School	12
Pupils using Mobile Phones in School	12

Staff using Work Devices Outside school	12
Monitoring and Review.....	13
Schedule for Monitoring, Review and Further Development	13
Related Policies	13
Useful references.....	14
Appendix 1: Process Flowchart	16
Appendix 2: Filtering and Monitoring Standards for Schools and Colleges.....	17
Appendix 3: Student Incidents and Actions.....	18
Appendix 4: Staff Incidents and Actions	20
Appendix 5: Why Your Online Reputation Matters.....	22
The Pillars of Good Netiquette.....	22

Purpose

Online Safety is an integral component of safeguarding at British School Quito helping to protect the school community from risks such as exposure to harmful content, cyberbullying, grooming and radicalisation. This policy helps ensure that students can access the benefits of the internet safely while minimising potential risks and harm.

Scope

This policy applies to all members of the school community (staff, students, parents, visitors, volunteers and other community users) who use school digital technology systems and networks, both in and out of the school.

Where the school places students with an alternative provision provider, it continues to be responsible for the safeguarding of those students. An assessment against this policy will be made with the provider, and the school should obtain written confirmation online safety controls are in place.

Legislation and Guidance

The Keeping Children Safe In Education (KCSIE) statutory guidance outlines definitions of online risks, including from AI and deepfake technologies.

Under the UK Education and Inspections Act 2006, Principals are reasonably empowered to regulate student behaviour off-site, and staff may impose disciplinary measures for misconduct, including online bullying, linked to school membership. The Education Act 2011 (Section 24b) extends these powers to include searching electronic devices and deleting data.

The school will address online misconduct through a range of policies and will inform parents when inappropriate online behaviour outside school is identified.

Types of Risks

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, including AI-generated images, audio or video.

Examples include pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, impersonation, misinformation, disinformation (including fake news) and conspiracy theories.

- **Contact:** being subjected to harmful online interaction with other users.

Examples include peer-to-peer pressure, commercial advertising or adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct:** online behaviour that increases the likelihood of, or causes, harm.

Examples include making, sending, receiving or sharing explicit images (both consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), harassment or online bullying

- **Commerce:** risks such as online gambling, inappropriate advertising, phishing or financial scams.

Inappropriate Content

The expectation is that:

- users are effectively and reliably prevented from generating or accessing harmful and inappropriate content
- filtering standards are maintained effectively throughout the duration of a conversation or interaction with a user
- filtering will be adjusted based on different levels of risk, age, appropriateness and the user's needs - for example users with special educational needs and disabilities (SEND)
- Multimodal content is effectively moderated, including detecting and filtering prohibited content across multiple languages, images, common misspellings and abbreviations
- Full content moderation capabilities are maintained regardless of the device used, including bring your own device (BYOD) and smartphones when accessing products via an educational institutional account
- Content is moderated based on an appropriate contextual understanding of the conversation, ensuring that generated content is sensitive to the context
- Filtering is regularly updated in response to new or emerging types of harmful content and AI tools users may access.

Roles & Responsibilities

All roles including external guests and must read and accept the acceptable use policy before accessing and using the schools' local and online systems and networks. The following responsibilities for online safety apply to specific roles:

School Board

- Approval of the Online Safety Policy
- Review the effectiveness of the policy based on feedback from the Regional Head of Schools (RHoS)

Regional Head of Schools (RHoS)

- Act as the Operational Board member responsible for Online Safety, which includes:
 - Holding regular meetings with the Designated Safeguarding Lead/Principal;
 - reviewing and approving any changes to the policy;
 - monitoring online safety incidents and reports;
 - reporting incidents to the Operational Board.

Principal and senior leaders

- Ensure the safety of the school community

- Ensure there is comparable authority/power under local legislation
- Ensure that there is a system in place for monitoring, reporting, and receiving incident reports from the Online Safety Officer/Designated Safeguarding Lead (DSL)
- Delegate day-to-day online safety responsibilities to the Designated Safeguarding Lead (DSL)
- Ensure all staff receive suitable training

DECE/Designated Safeguarding Lead (or Deputy)

- Lead the Online Safety Group – as part of the Safeguarding Team Meetings
- Manage day-to-day online safety incidents, and maintains a record of all incidents
- Review process and policy and suggests improvements or non-compliance to the leadership team
- Provide training and advice to all staff
- Liaise with technical staff and external authorities

Network/IT Manager and technical staff

- Stay up-to-date with regard to online safety policy, practice and training
- Ensure the physical security of the school's technical infrastructure
- Implement and monitor online safety measures and ensure they are up-to-date, including firewall and anti-virus protection
- Ensure all technology related to online access is protected in line with local regulations, the Online Safety Policy and group baselines
- Ensure any contracted third-party suppliers follow the online safety measures and are fully aware of the schools' processes before working in the school
- Ensure that any messaging and collaboration platforms are monitored for misuse and, in the event of an incident, report to the Online Safety Officer and senior leadership team for investigation
- Ensure that physical access to IT systems is restricted to the appropriate level and that users have clearly defined access rights (this includes online and removable storage, staff and student data systems, organisational data and internet access).
- Ensure that all students and staff are provided with a username and password that meets security standards outlined in the Password Policy, and that no generic user accounts are in use in any school systems.
- Ensure that all master admin usernames and passwords are stored in an encrypted vault, and that the Principal has access to this in case of emergencies for business continuity.
- Ensure that all software licenses are up to date and cover the number of users/ devices in use in the school.
- Ensure that all internet access is filtered to the appropriate age and role level in the school, that the firewall and security gateways are up-to-date, and that the security controls reflect the safeguarding controls outlined in the Safeguarding Controls Policy.
- Support the Online Safety Officer/DSL in ensuring that a system is in place to monitor, record and report online safety incidents.
- Ensure that the Acceptable Use of IT Policy is available to staff, students, parents and third-party collaborators, and is enforced **before** access is granted to school systems and networks.
- Conduct an annual cyber risk assessment, and review this each term
- Develop and implement a plan to back up the school's data and review this each year
- Report all cyber attacks

Teaching and Support Staff

- Read, understand and comply with the Online Safety and Acceptable Use of IT policies
- Stay updated about online safety matters
- Embed online safety in the curriculum
- Monitor and guide the students' use of digital technologies
- Report any misuse to the Online Safety Officer and senior leadership team for investigation
- Ensure that all communications with students and parents are made using official school systems, and that conversations are always of a professional nature
- Ensure students understand the Online Safety Policy and how to avoid plagiarism and copyright infringement
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use, ensuring processes are in place for dealing with any unsuitable material that is found in internet searches
- monitor and implement current policies regarding devices whenever the use of digital technologies, mobile devices, cameras, etc. is allowed in lessons and other school activities

Students

- Understand the Online Safety and Acceptable Use of IT policies
- Use school digital technology systems responsibly, following the Acceptable Use of IT Policy
- Report misuse or inappropriate materials
- Follow guidance on good practice, taking images safely, appropriate mobile phone use, and develop an understanding of online bullying

Parents

- Support the school's online safety policies
- Monitor their children's online activities
- Understand the importance of good online safety and what it looks like, with particular regard to:
 - good personal device use
 - digital photo and video images at and around school events
 - safe access and sharing guidance on parents' sections of learning platforms and online student records

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 3).

Education and Training

While regulation and technical measures are important, educating students to act responsibly online is essential. Online safety and digital literacy are key parts of the school's provision, helping students recognise risks and build resilience. Online safety should be integrated across the curriculum, with staff reinforcing key

messages. The curriculum for online safety should be broad, age-appropriate, and offer progression through creative learning opportunities, tailored to the school's structure and student age groups.

Students' Education

To ensure a consistent and effective approach to online safety, the school will implement the following measures:

- **Curriculum Delivery:** A structured online safety curriculum will be delivered through Computing, PSHE, and other relevant subjects, with regular reinforcement.
- **Whole-School Messaging:** Key online safety messages will be embedded in assemblies, tutorials, and pastoral programmes.
- **Critical Thinking:** Students will be taught to critically evaluate online content and verify its accuracy.
- **Digital Responsibility:** Lessons will include guidance on acknowledging sources and respecting copyright.
- **Resilience to Radicalisation:** Students will be supported in developing resilience through safe discussions of controversial topics and understanding civic participation as opposed to extremism.
- **Acceptable Use:** Students will be educated on the importance of the Acceptable Use of IT Policy and encouraged to use technology responsibly in and out of school.
- **Staff Role Modelling:** Staff will model appropriate use of digital technologies, the internet, and mobile devices.
- **Safe Browsing Practices:** In pre-planned internet use, students will be directed to vetted websites, and procedures will be in place to manage exposure to unsuitable content.
- **Monitoring:** When students have open internet access, staff will actively monitor their activity.
- **Access to Restricted Content:** For legitimate educational purposes (e.g. research on racism, drugs, discrimination), staff may request temporary access to blocked sites. Such requests must be auditable and justified, and may be approved by the Principal, in consultation with the RHoS where necessary.

Primary School

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of Primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Secondary school

In **KS3**, 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

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of Secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another 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 shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is 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
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable pupils as required.

Parent Education and Engagement

Parents play a vital role in guiding and monitoring their children's online behaviour, yet many may be unaware of the risks or how to respond to online safety concerns. To support parents, the school will raise awareness and provide regular information through:

- curriculum-linked activities
- communications (e.g. letters, newsletters, website, learning platform)
- parent sessions, workshops and events
- campaigns (e.g. Safer Internet Day)
- signposting to trusted resources (e.g. saferinternet.org.uk, childnet.com)
- providing information and resources to support online safety at home
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of School and/or the DECE DSL.

Staff/Volunteers Education and Engagement

- All staff receive regular formal, audited online safety training as part of their CPD and mandatory training plan
- New staff receive online safety training as part of their induction, completed within the first 3 weeks
- All staff review and formally agree with the Online Safety Policy and other related policies as part of start-of-year activities or in-year induction

Regional Head of Schools (RHoS) and School Board

- Participate in regular formal, audited Online Safety training as part of their CPD and mandatory training plan

Dealing With Incidents of Misuse

This section covers the steps required to deal with incidents and aims to ensure that:

- clear procedures for handling incidents are followed; and
- immediate reporting of serious incidents is made to the appropriate authorities.

Incidents

When investigating incidents, school leaders will:

- involve at least two senior staff, to ensure accountability;
- use a designated computer not accessible to students. This device may be required by police;
- ensure the investigators have monitored and recorded internet access;
- maintain a timeline of events for potential police reporting;
- record URLs and describe concerning content. The capture and storing of screenshots may be beneficial, but must exclude images of child abuse;

After investigation, the school leaders will determine if the concern is valid and take appropriate action:

- internal disciplinary measures;
- referral to the Regional Head of Schools and/or other relevant authorities;
- police involvement.

Mandatory Police Referral

Certain incidents must be reported to the police without exception:

- child abuse imagery
- grooming behaviour
- sending obscene materials to a child
- breaches of the Obscene Publications Act
- criminally racist content
- promotion of terrorism or extremism
- other criminal activities

Safeguarding Measures

- The computer used for investigation should be isolated, to preserve evidence and avoid the chance of tampering.
- All steps followed should be recorded in a chronological log to create a clear evidence trail for safeguarding and legal purposes.
- The completed investigation form/log must be retained for reference.

Actions and Sanctions

It is important that any incidents are dealt with as soon as possible, and in a proportionate manner. It is also important that members of the school community are aware that incidents have been dealt with.

A process flowchart and suggested actions and sanctions for incidents are included in the Appendix.

Cyber-bullying

Definition

Cyber-bullying 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 1 person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, 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 they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their tutor groups.

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

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DECE / DSL 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 it is deemed necessary to do so.

Examining Electronic Devices

Staff 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 in relation to 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:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Principal / Head of School / DSL / appropriate staff member.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- 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.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DECE DSL will decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image

- Confiscate the device and report the incident to the DSL DECE immediately, who will decide what to do next. The DSL will make the decision in line with the latest Ecuadorian guidance.

Any searching of pupils will be carried out in line with Ecuadorian law with regard to:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- BSQ behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

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 Bard.

We recognise that AI has many uses to help pupils learn but may also have the 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.

The use of AI to create videos, photos, voices or any other documents is strictly prohibited. We will treat any use of AI to bully pupils in line with our anti-bullying & behaviour policy, and modify this policy as more information, guidance and direction becomes available.

Acceptable Use of the Internet in School

All pupils, parents/carers, staff, are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. Virtual Private Networks must not be used in school.

We will monitor the websites visited by pupils and staff to ensure they comply with the above and restrict access through filtering systems where appropriate.

Pupils using Mobile Phones in School

The use of mobile phones in school is not allowed under any circumstances. Emergency communication will be through standard school channels.

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:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

Monitoring and Review

This policy has been developed by a working group comprising:

- Principal / Senior Leader Team
- Online Safety Officer / Designated Safeguarding Lead (DECE)
- Staff (Teachers, Support Staff, Technical Staff)
- Regional Head of Schools / Board
- Parents
- Student Representatives

Schedule for Monitoring, Review and Further Development

- V1 Approval: By the Board on 31/07/2025
- Monitoring: By the Senior Leadership Team, at least annually
- Reporting: Annually to the Regional Head of Schools (RHoS) and the Board, with immediate reporting for serious incidents
- Review: Annually, or as needed based on new developments or following incidents, by RHoS on behalf of the Board

Related Policies

This policy should be read in conjunction with the following documents:

- Child Protection and Safeguarding Policy
- Anti Bullying Policy
- Behaviour Policy
- Staff Code of Conduct Policy
- Concerns and Complaints Procedure
- Acceptable Use of IT Policy Primary
- Acceptable Use of It Policy Secondary

Useful references

UK Safer Internet Centre: saferinternet.org.uk - [guides and resources](#)

- *In particular, the UK Safer Internet Centre has produced a series of webinars for teachers on behalf of the DfE to inform and support schools with their filtering and monitoring responsibilities - [Appropriate Filtering and Monitoring](#)*

UK government: [Education, training and skills - gov.uk](#)

- [Filtering and Monitoring Standards](#)
- [Cyber security standards for schools and colleges](#) developed to help them improve their resilience against cyber-attacks
- [Preventing Bullying](#) (includes cyberbullying)
-

- [Information sharing for people who provide safeguarding services to children](#)

UK Council for Internet Safety: [UKCIS](#)

- [Sharing nudes and semi-nudes](#) advice for schools and colleges on responding to incidents of consensual and non-consensual sharing of nudes and semi-nudes.

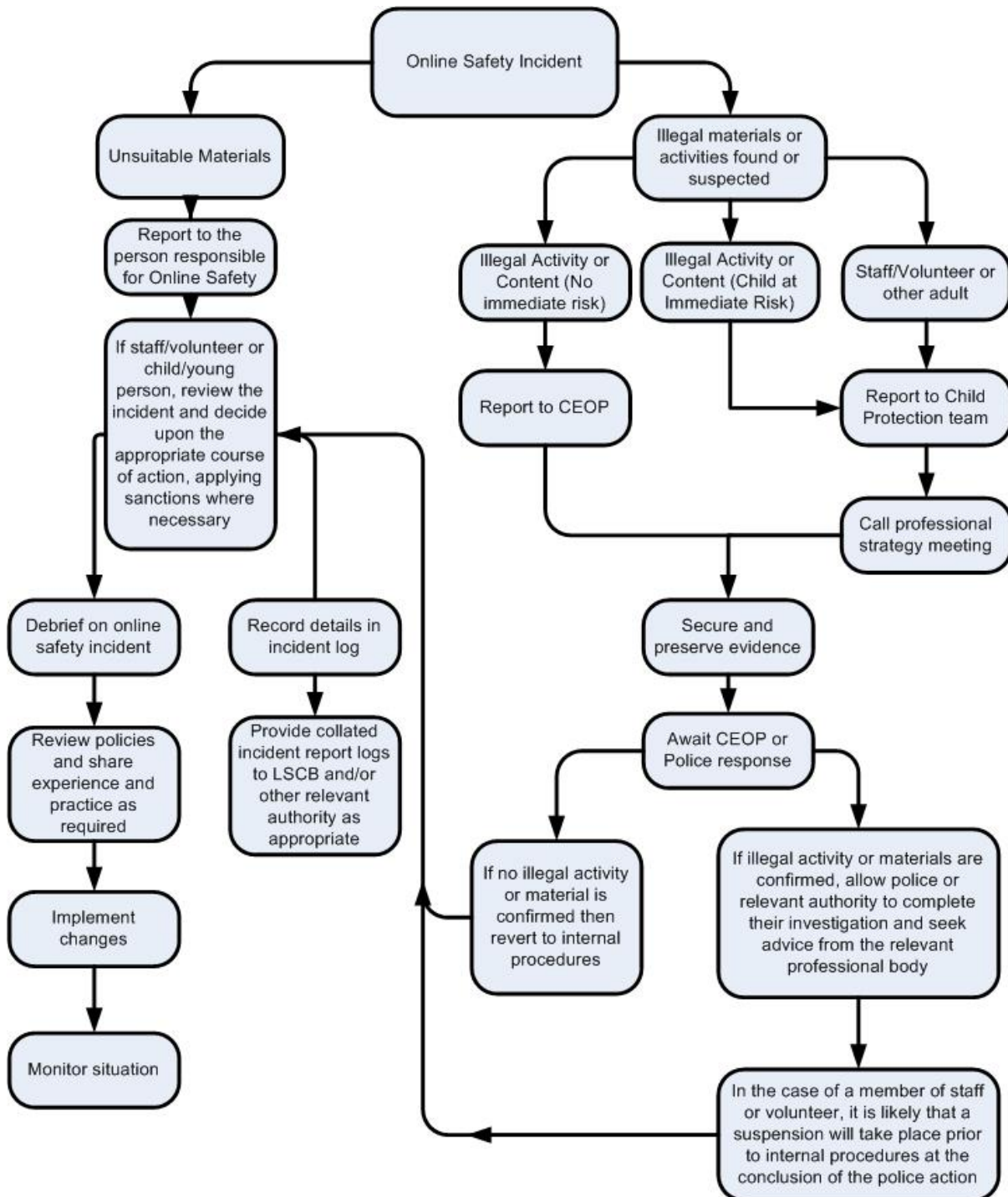
Childnet: [Childnet](#)

- [Just a joke?](#) – lesson plans, activities, a quiz and teaching guide designed to explore problematic online sexual behaviour with 9-12 year olds.

Information Commissioner's Office: [GDPR guidance and resources](#)

- [Data-sharing information hub](#) – resources to help schools and colleges comply with data protection legislation including UK GDPR.

Appendix 1: Process Flowchart



Appendix 2: Filtering and Monitoring Standards for Schools and Colleges

As a school we use [watchguard](#) as our filtering and monitoring system ensuring our cyber security. We clearly meet the [filtering and monitoring standards for schools](#) as published by the British Government

David Chandos our IT lead has responsibility to manage our filtering and monitoring systems. He works with the DECE DSL and the Principal to ensure our systems remain fir for purpose in real time.	✓
Our filtering and monitoring system is reviewed and updated as required, and at a minimum annually	✓
Our filtering system blocks harmful and inappropriate content, without unreasonably impacting on teaching and learning.	✓
We have effective monitoring strategies that meet the safeguarding needs of our school.	✓

Appendix 3: Student Incidents and Actions

Scenario	Action 1	Action 2	Action 3	Action 4	Action 5
Unauthorised downloading or uploading of files	warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Continued infringements of the above, following previous warnings or sanctions	further sanction e.g. detention / exclusion	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
<u>Accidentally</u> accessing offensive or pornographic material and failing to report the incident	warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
<u>Deliberately</u> accessing or trying to access offensive or pornographic material	suspension	removal of network / internet access rights	refer to Principal	inform parents / carers	refer to Police
Deliberately accessing or trying to access material that could be considered illegal	suspension	removal of network / internet access rights	refer to Principal	inform parents / carers	refer to Police
Using proxy sites or other means to subvert the school's filtering system	disciplinary action	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	disciplinary action	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Breaching copyright or licensing regulations	warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Corrupting or destroying the data of other users	disciplinary action	removal of network / internet access rights	refer to Principal	inform parents / carers	refer to Police
Careless use of personal data e.g. holding or transferring data in an insecure manner	warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Allowing others to access school network by sharing username and passwords or attempting	disciplinary action	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–

Scenario	Action 1	Action 2	Action 3	Action 4	Action 5
to access or accessing the school network, using another person's account					
Deliberate actions to breach data protection or network security rules	disciplinary action	removal of network / internet access rights	refer to Principal	inform parents / carers	refer to Police
Inappropriate personal use of the internet / social media / personal email	warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	-
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	disciplinary action	removal of network / internet access rights	refer to Principal	inform parents / carers	refer to Police

Appendix 4: Staff Incidents and Actions

Scenario	Action 1	Action 2	Action 3	Action 4	Action 5
Actions which could compromise the staff member's professional standing	disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
Unauthorised downloading or uploading of files	warning	disciplinary action	suspension	refer to Principal	refer to RHoS / HR
Continued infringements of the above, following previous warnings or sanctions	disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
<u>Accidentally</u> accessing offensive or pornographic material and failing to report the incident	warning	disciplinary action	refer to Principal	refer to RHoS / HR	
<u>Deliberately</u> accessing or trying to access offensive or pornographic material	suspension	refer to Principal	refer to RHoS / HR	refer to Police	
Deliberately accessing or trying to access material that could be considered illegal	suspension	refer to Principal	refer to RHoS / HR	refer to Police	
Using proxy sites or other means to subvert the school's filtering system	disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
Breaching copyright or licensing regulations	warning	disciplinary action	suspension	refer to Principal	refer to RHoS / HR
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	disciplinary action	suspension	refer to Principal	refer to RHoS / HR	refer to Police
Careless use of personal data e.g. holding or transferring data in an insecure manner	warning	disciplinary action	refer to Principal	refer to RHoS / HR	
Allowing others to access school network by sharing usernames and passwords or attempting to access or accessing the school network, using another person's account	disciplinary action	suspension	refer to Principal	refer to RHoS / HR	

Scenario	Action 1	Action 2	Action 3	Action 4	Action 5
Deliberate actions to breach data protection or network security rules	disciplinary action	suspension	refer to Principal	refer to RHoS / HR	refer to Police
Inappropriate personal use of the internet / social media / personal email	warning	disciplinary action	refer to Principal	refer to RHoS / HR	
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students	disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	disciplinary action	suspension	refer to Principal	refer to RHoS / HR	refer to Police

Appendix 5: Why Your Online Reputation Matters

- **First Impressions are Lasting:** In an era where many interactions begin online, potential employers, clients, or even acquaintances often research individuals before making contact. A strong, positive online reputation can open doors, while a negative one can close them before they even have a chance to be seen.
- **Career Advancement and Opportunities:** A significant percentage of employers' screen candidates by reviewing their social media profiles and online presence. A professional and respectful digital persona can enhance career prospects, while inappropriate content or behaviour can lead to missed opportunities or even job loss.
- **Building Trust and Credibility:** A well-managed online reputation fosters trust and establishes credibility. It demonstrates reliability, responsibility, and authenticity, which are valuable assets in any field. Positive reviews and a consistent, professional online presence can significantly influence consumer trust and business success.
- **Personal and Professional Relationships:** Your online interactions can impact your real-world relationships. Thoughtless or disrespectful comments can alienate friends, family, and colleagues, while constructive and considerate engagement can strengthen bonds.
- **Safeguarding Against Negative Consequences:** A strong online reputation acts as a protective shield against issues like cyberbullying, identity theft, and doxxing. By controlling the information available about you and maintaining a positive digital narrative, you can mitigate these risks.
- **The Permanence of the Digital World:** Content shared online can be difficult to erase. Mistakes, misinformation, or regrettable posts can resurface years later, potentially affecting future opportunities and relationships.

The Pillars of Good Netiquette

Netiquette provides the framework for respectful and constructive online interactions. Adhering to these unwritten rules is paramount:

- **Remember the Human:** Always keep in mind that you are communicating with real people who have feelings. Avoid the temptation to be overly blunt or aggressive online, as you would not in person.
- **Adhere to Real-Life Standards:** The same courtesy, respect, and honesty you practice offline should extend to your online behavior.
- **Respect Others' Time and Bandwidth:** Be concise and relevant in your communications. Avoid sending large, unnecessary files or overwhelming others with excessive messages.
- **Communicate Respectfully:** Refrain from using offensive language, name-calling, or expressing deliberately provocative opinions. Ensure your tone is appropriate for the platform and audience.
- **Maintain Professionalism:** Especially in professional contexts, ensure your online presence reflects positively on you and your organization. This includes using proper grammar and spelling, avoiding excessive slang, and presenting a polished image.
- **Know Your Audience and Platform:** Understand the norms and expectations of different online spaces. What might be acceptable on a personal blog could be inappropriate for a professional forum.
- **Protect Privacy:** Respect the confidentiality of others and safeguard your own personal information. Be transparent about data usage and ensure secure practices.
- **Fact-Check and Share Responsibly:** Before sharing information, especially news or opinions, verify its accuracy to avoid spreading misinformation.

- **Be Mindful of Tone:** Written communication can easily lead to misunderstandings. Reread your messages to ensure your intended tone is conveyed clearly and respectfully.
- **Embrace Imperfection:** Mistakes happen. When they do, acknowledge them, learn from them, and strive to do better.

By actively practicing good netiquette and consciously managing your online reputation, you cultivate a positive digital presence that supports your personal growth, professional success, and overall well-being in an increasingly digital world.