British School Quito
an Orbital Education School

All our polices are developed to ensure our values are at the centre of all we do, as we work in the best interests of our pupils to ensure the best outcomes for them. All polices can be updated out with the set review cycle if advice, guidance, or new learning require it.

Excellence ***Excelencia***	***Respect*** ***Respeto***	***Responsibility*** ***Responsabilidad***	***Integrity*** ***Integridad***	***Compassion*** ***Compasión***

We live and learn together:

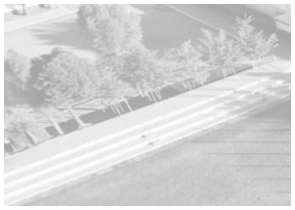
1. with **respect** and **care** for each other
2. with a **happy** and **welcoming** attitude to everyone
3. with an **active** and **determined** approach to our ambition

Online Safety Policy

Adopted:	Monday, 01 September 2025
Review cycle:	1 Year review cycle.
Next review:	Tuesday, 01 September 2026
Policy Lead:	Designated Safeguarding Lead.

Published:	Policy SharePoint:	✓	BSQ Website:	✓




Contents

Aims

At BSQ we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others

- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 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, self-harm, suicide, antisemitism, radicalisation and extremism
- **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 with the intention 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 sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying;
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

British guidance that informs our practice

This policy is based on the Department for Education's (DfE's) safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying
- cyber-bullying: advice for headteachers and school staff
- Protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The governing board via the Regional Head of schools

The Regional Head represents the Governing Body and has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Regional Head will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Regional head will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The regional Head will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Regional Head should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Regional Head must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The regional head will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

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

If applicable, add: The Regional Head who oversees online safety 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 3)
- 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). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The DECE Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher 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 ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager 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 child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (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 headteacher 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, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The ICT Lead

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess 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 monitoring the school's ICT systems on a [weekly/fortnightly/monthly] basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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

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
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet
- Knowing that the DSL 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 [insert school specific action here]
- Following the correct procedures by [insert school specific action here] if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher 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 (appendices 1 and 2)
- To understand the importance of their childs on line reputation (their netiquete)

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
- Parent resource sheet – Childnet

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).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

We teach:

- Understanding the importance of maintaining a good online reputation (netiquete)

Primary schools

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 schools

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.

Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in communications home, and in information via our website. This policy will also be shared with parents/carers via our website.

The school will let parents/carers know:

- What systems the school uses 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

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.

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 headteacher / 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 Ecuadorain 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
- Our 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.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

The DECE DSL and the wider safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Links with other policies in SharePoint library

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Anti Bully policy
- Behaviour policy
- Staff conduct and disciplinary policy
- Concerns and Complaints procedure
- ICT and internet acceptable use policy primary
- ICT and internet acceptable use policy secondary

Appendix 1.

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 anually	✓
Our filtering system blocks harmful and inappropriate contet, without unreasonably impacting on teaching and learning.	✓
We have effective monitoring strategies that meet the safeguarding needs of our school.	✓

Appendix 2

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 behavior 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.