CAPITAL SCHOOL BAHRAIN

Online Safety Policy

DOCUMENT CONTROL	
Policy Reference	CSB – Online Safety Policy
Date Adopted	August 2025
Last Review Date	June 2025
Next Scheduled Revision (yearly)	June 2026

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and the wider school community
- 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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; sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

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

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

Capital School Bahrain also adheres to all Bahraini national legislation and guidance from the Ministry of Education and other national statutory agencies.

3. Roles and responsibilities

3.1 The Principal

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

3.2 The deputy designated safeguarding lead (DDSL)

Details of the school's deputy designated safeguarding lead (DDSL) is set out in our Safeguarding Policy, as well as relevant job descriptions.

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

- Supporting the Principal in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal and senior leadership to review this policy and make sure 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 IT staff to make sure the appropriate systems and processes are in place
- Working with the Principal, IT staff 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
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal
- Undertaking annual risk assessments that consider and reflect the risks pupils 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.

3.4 The IT department

The IT department 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 make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's IT 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 IT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Making sure 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.

3.5 All staff and volunteers

All staff, including contractors and 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 and making sure that pupils follow the school's ICT Acceptable Use Policy
- Knowing that the DDSL 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.
- Following the correct procedures by reporting to the Principal and/or DDSL if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DDSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure 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.

3.6 Parents/guardians

Parents/guardians are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet

3.7 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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating parents/guardians about online safety

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

Online safety will also be covered during inputs by staff.

The school will let parents/guardians 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/guardians have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DDSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

5. Cyber-bullying

5.1 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. (See also the school behaviour policies.)

5.2 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 encourage them 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.

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 and volunteers (where appropriate) 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 DDSL 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.

5.3 Examining electronic devices

The Principal, 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 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 DDSL and the Principal
- Explain to the pupil why they are being searched, and 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 Principal, DDSL and/or Senior Leadership to 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 whether 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

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

5.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/guardians may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Capital School Bahrain recognises 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Capital School Bahrain will treat any use of AI to bully pupils seriously, and all matters will be dealt with in accordance with our **Anti-Bullying Policy**.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the School, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our Artificial Intelligence Policy.

6. Acceptable use of the internet and IT in school in school

All pupils, staff, volunteers, parents/guardians and the wider school community are expected to use the internet and IT assets in accordance with our **ICT Acceptable Use Policy**.

7. 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 can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- 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 promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's ICT Acceptable Use Policy.

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 IT staff.

8. 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 ICT Acceptable Use and the school's Behaviour Policies. 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 HR Policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. Training

9.1 Staff and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

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

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 DDSL 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. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our Safeguarding Policy.

9.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

10. Monitoring arrangements

The DDSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

11. Links with other policies

This Online Safety Policy is linked to our:

- Safeguarding Policy
- Behaviour Policies
- Data Protection Policy
- Anti-Bullying Policy
- Complaints Policy
- ICT Acceptable Use Policy
- Artificial Intelligence Policy