CAPITAL SCHOOL BAHRAIN

ICT Acceptable Use Policy

DOCUMENT CONTROL	
Policy Reference	CSB - ICT Acceptable Use Policy
Date Adopted	August 2025
Last Review Date	June 2025
Next Scheduled Revision (yearly)	June 2026

Table of Contents

1. Introduction 3
2. Responsibilities 3
3. Security 4
4. Capital School Bahrain Network 4
5. Capital School Bahrain Email – Outlook 5
6. Internet 6
7. Electronic Devices (School-Owned & BYOD) 8
8. Cyberbullying 9
9. Radicalisation 10
10. Use of Other Technology 10
11. Education and Awareness 10
12. Disciplinary Procedures 11

1. Introduction

1.1. The purpose of the ICT Acceptable Use Policy is to ensure that pupils at Capital School Bahrain are able to take advantage of the potential of ICT to support and enhance their learning in a responsible and secure manner. This policy aims to set guidelines and rules on the use of school ICT resources for staff, pupils, parents/guardians and those who come into contact with Capital School Bahrain and our ICT infrastructure. This policy establishes clear expectations for the way all members of the school community engage with each other online and is intended to prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems and support the school in teaching pupils safe and effective internet and ICT use.

1.2. This policy applies to all relevant digital devices - not just desktops and laptops - but also smartphones, tablets and wearable devices are applicable. The policy applies to both School and privately-owned equipment brought on site by either pupils, staff or third parties, as well as School and privately owned equipment used to access Capital School Bahrain services and data.

1.3. Capital School Bahrain believes in the educational benefits that can be offered to pupils through the correct and appropriate use of technology. However, it is acknowledged there is a need to address the dangers and raise awareness of potential abuses of technology. Good planning and management at Capital School Bahrain will ensure appropriate and effective staff and pupil use.

1.4. This policy is designed primarily to safeguard pupils, but also to provide guidance for adults in positions of responsibility. It applies to all members of Capital School Bahrain community, including pupils, teachers, support staff, visitors, volunteers and temporary staff/contractors. It is not limited to the school network; it is designed to cover all aspects of Online Safety that may impact on the school community. The policy also includes the usage of all forms of ICT, including but not limited to computers, laptops, tablets, smartphones, virtual reality (VR) equipment, and software applications – both provided by the school and personal devices/software used on-site or as a part of wider CSB obligations.

1.5. The safe and appropriate use of technology is not a standalone issue. This policy should be read in conjunction with all other policies.

1.6. To ensure this outcome, our pupils and their parents need to understand the rules and systems that we have put in place to protect our users and school system.

2. Responsibilities

2.1. Senior Leadership will ensure both the Acceptable Use of ICT Policies and related policies are implemented. These policies will be reviewed during the course of each academic year or post any specific technological developments by the IT Department, prior to being endorsed by the Digital Learning Strategy & AI Integration Lead and approved in final by the Principal.

2.2. All users of digital technology at Capital School Bahrain are expected to act responsibly and to show consideration to others.

2.3. It is not acceptable to:

2.3.1 Install, download, or run unauthorised software, apps, or games on any school-owned device.

2.3.2 Introduce, create, or distribute malware, viruses, or other malicious code.

2.3.3 Attempt to bypass, disable, or interfere with any security, filtering, or monitoring controls.

2.3.4 Use, share, or attempt to access another person's account, credentials, or files.

2.3.5 Attempt to access any system, service, data, or location without explicit authorisation.

2.3.6 Use hacking, cracking, password-recovery, packet-sniffing, or similar tools.

2.3.7 Connect unauthorised network equipment (e.g., routers, switches, wireless APs) or create hotspots/tethering; using cellular data (3G/4G/5G) to circumvent school controls on site is prohibited.

2.3.8 Access, create, store, transmit, or share material that is indecent, obscene, harassing, hateful, infringing (e.g., copyright), or otherwise unlawful.

2.3.9 Deliberately waste IT support time or school technical resources.

2.3.10 Bring food or drink into ICT rooms or near school devices/equipment.

2.3.11 Damage, tamper with, or interfere with any device, cable, peripheral, or network equipment.

2.3.12 Share internal school materials, data, or resources with any person or service outside Capital School Bahrain without permission.

2.3.13 Record (video or audio) online lessons, meetings, or events without prior authorisation.

2.3.14 Capture screenshots or photographs of online lessons, meetings, or events without prior authorisation.

2.3.15 Browse, download, upload, forward, or otherwise distribute content that is offensive, inappropriate, or illegal.

2.3.16 Share meeting links, invites, or access codes (e.g., Teams/Zoom/Meet) with unauthorised individuals.

2.3.17 Use VPNs, proxies, or similar services to access blocked sites/services (including gaming and streaming) or to evade monitoring/filtering.

2.3.18 Use ICT tools—including AI, AR/VR, or automation—in any unauthorised, unsafe, or inappropriate manner.

3. Security

3.1 Each user is responsible for keeping their login details secure and must not share their username or password with anyone else.

3.2 Users must only access systems, data, or devices assigned or authorised for their use.

3.3 No user should attempt to log in as someone else or use a device or account that has been logged in by another person.

3.4 Users who leave their workstation or device unattended for more than a short period must lock or log off their session to prevent unauthorised access.

3.5 Internet access is filtered and monitored to help protect users and school systems from harmful or inappropriate content. All online activity on school networks and systems may be logged and reviewed in accordance with safeguarding and data protection policies.

3.6 Users must respect copyright and intellectual property laws when accessing, copying, or using material from the internet or digital platforms.

3.7 Photographs, videos, or recordings of any pupils, staff, or visitors must not be taken, stored, or shared without their explicit written consent (and, in the case of pupils, parental/guardian permission).

3.8 Users should be aware that the school reserves the right to access school-managed folders, emails, and accounts if there is reason to believe that this policy or related school guidelines have been breached. While privacy will be respected, monitoring may occur to maintain the safety, integrity, and lawful use of school systems.

4. Capital School Bahrain Network

4.1. Capital School Bahrain is committed to maintaining a safe, secure, and reliable digital environment. Internet content is filtered to reduce access to material that is offensive, inappropriate, illegal, harmful, or that promotes extremism or radicalisation. These filters are reviewed regularly; however, no system can guarantee complete protection, and inappropriate content may occasionally be accessible.

4.2. Users should be aware that creating or using personal mobile hotspots, tethering, or connecting through unfiltered mobile data services (e.g. 3G, 4G, 5G) to bypass school network controls is strictly prohibited. Such activity undermines the school's safeguarding and monitoring procedures and will be treated as a serious breach of this policy.

4.3. The school cannot accept liability for material accessed, nor for any consequences arising from internet use. All users are responsible for their actions when using digital systems, networks, and online services.

4.4. Pupils receive guidance and training on how to stay safe online, how to recognise and respond to inappropriate content or contact, and how to report any concerns. All users are expected to adhere to the Acceptable Use Policy and act as positive digital citizens.

4.5. Every authorised user is issued a unique username and password with clearly defined access rights. The school monitors digital activity, communication, and online behaviour to help ensure the network remains safe, secure, and used appropriately.

4.6. All staff are expected to follow the school's safeguarding policies when using technology, whether on the school network or external platforms. The principles of Prevention, Protection, and Support must guide all staff actions related to online conduct, communication, and pupil wellbeing.

5. Capital School Bahrain Email – Outlook

5.1 All Capital School Bahrain staff and pupils are provided with a school-issued email account for educational and professional use.

5.2 Pupils receive guidance on how to use email responsibly and effectively as a communication tool.

5.3 All email communication must be appropriate, professional, and supportive of the school's values and reputation.

5.4 School email is monitored and filtered for safety, security, and safeguarding purposes. Users should understand that emails sent or received via school systems may be accessed or reviewed by authorised personnel or, where required, external agencies.

5.5 Messages containing sensitive or confidential information for parents or external recipients must be reviewed and approved by the Principal before sending.

5.6 Each user is accountable for all activity conducted through their assigned email account.

5.7 The use of third-party or personal email services on school premises is discouraged and may be restricted. Excessive personal use of email during school hours is not permitted.

5.8 For safeguarding reasons, staff should only communicate with pupils through official school email accounts unless approved otherwise by a senior leader.

5.9 Do not open attachments or click links from unknown or suspicious senders. If this occurs, shut down the device immediately and notify the Digital Learning Strategy & AI Integration Lead and the IT Department.

5.10 Never share personal details (such as address, phone number, or passwords) via email, and never agree to meet unknown contacts.

5.11 All email messages should use appropriate, polite, and professional language.

5.12 Chain letters, spam messages, or mass forwarding are not permitted.

5.13 Staff must report any offensive, threatening, or inappropriate emails to their line manager or a member of the Senior Leadership Team and should not attempt to handle such incidents independently.

5.14 Pupils must inform a teacher or trusted staff member if they receive any offensive, threatening, or unsuitable emails and should not reply to or delete them.

6. Internet

6.1. The purpose of internet access at Capital School Bahrain is to enhance learning, raise educational standards, support staff in their professional work, and strengthen the school's management and communication systems.

6.2. Internet use is an essential part of modern education. Pupils and staff are entitled to access it responsibly, provided they use it for legitimate educational or professional purposes.

6.3. Unauthorised or inappropriate use of the school network, systems, or devices is strictly prohibited and may constitute a disciplinary or criminal offence.

6.4. Internet access is filtered and monitored to block harmful, illegal, or inappropriate material. Filters are reviewed regularly; however, complete protection cannot be guaranteed, and users must report any unsuitable content immediately.

6.5. The use of unfiltered third-party connections (e.g. mobile hotspots, dongles, or tethered smartphones) to bypass school security systems is prohibited. The school may inspect any device connected to the network to ensure compliance and security.

6.6. All internet-enabled devices brought onto the premises must have approved antivirus protection installed and kept up to date.

6.7. Pupils receive guidance and education on safe and responsible internet use. Staff are expected to model appropriate online behaviour at all times.

6.8. Social Media & Online Presence:

6.8.1 Social networking sites (e.g. Facebook, X/Twitter, Instagram, TikTok, LinkedIn etc.) must be used responsibly and never in a way that brings the school or its community into disrepute.

6.8.2 Any direct or indirect reference to the school, its staff, or pupils must be respectful, accurate, and appropriate. The school reserves the right to request the removal of any content it considers inappropriate.

6.8.3 Pupils are taught how to use social media safely, including protecting their privacy, avoiding oversharing, and using nicknames or avatars when appropriate.

6.8.4 Access to social networking platforms is generally blocked for pupils, unless a specific educational purpose is approved by Senior Leadership.

6.8.5 Staff must not use social media to communicate with pupils or parents regarding school matters.

6.8.6 Pupils and staff should avoid posting personal or emotional content that could be interpreted as harmful, defamatory, or unprofessional.

6.8.7 All members of the school community are reminded that their online conduct reflects on Capital School Bahrain and should therefore uphold the school's standards and values at all times.

6.9. Safe and Appropriate Internet Access:

6.9.1 Not all material online is suitable for pupils. The school supervises access and takes reasonable precautions to ensure users encounter only age-appropriate resources.

6.9.2 Staff must check that websites and online resources are appropriate for the age and maturity of pupils before use.

6.9.3 Filtering levels are adjusted based on user role; pupils receive stricter filtering than staff.

6.9.4 Pupils must never make online purchases or enter payment information using school systems.

6.9.5 Any discovery of inappropriate material or misuse of the internet must be reported promptly to the IT Department.

6.9.6 The school reviews its online safety measures annually to identify risks and ensure continued protection.

7. Electronic Devices (School-Owned & BYOD)

Purpose and conduct

- Devices are learning and work tools. During school hours and on school networks, use them for educational or professional tasks only.
- Accessing harmful, inappropriate, or non-curricular social media/gaming sites is not permitted.

When and how to use

- Use devices when directed by a teacher or, for staff, as required for your role.
- Follow classroom and lab rules at all times.

Photos, video, and audio

- Do not record, photograph, or share images/audio/video of pupils, staff, or parents without prior authorisation and the required consents.
- Never record or photograph pupils, staff or parents on a personal device.
- Inappropriate or unauthorised recording or sharing will lead to disciplinary action.

Security and safety

- Do not try to bypass filtering, monitoring, or management controls. VPNs, personal hotspots/tethering, or other methods to evade school controls are not allowed on site.
- Only connect to approved school networks. Do not attach any network hardware (e.g., routers, access points, switches).

Care and supervision

- Keep devices safe and never leave them unattended.
- Transport and store them securely (e.g., in a case); keep food and drink away from equipment.

Confiscation and inspection

- If there is a safeguarding, security, or policy concern, authorised staff may temporarily confiscate a device and/or make a limited inspection to check compliance.

School-Owned / Loaned Devices

- Remain the property of the school and may include management profiles, filtering, and security software. Do not remove or tamper with these controls.
- Do not take school devices to external repair shops. Report faults to the IT Department.
- Report loss, theft, or damage immediately. After investigation, the user/parent may be charged part or all repair/replacement costs where wilful damage or negligence is found.

BYOD (Personally-Owned Devices Used for School)

- Must meet the published BYOD specifications and allow required security/management tools (e.g., endpoint protection, classroom management agent, certificates) while used on school networks or for school work.
- Owners are responsible for maintenance, insurance, and repairs. The school is not liable for loss, theft, or damage to these devices.
- BYOD use is subject to the same filtering, monitoring, and behaviour standards as school devices when connected to school services.
- Personal hotspots/tethering must not be used to bypass school controls; use approved school Wi-Fi only.
- Where there are serious safeguarding or compliance concerns, the school may request a limited inspection to verify required settings/agents are in place.

8. Cyberbullying

8.1. Capital School Bahrain has a zero-tolerance approach to bullying in any form; cyberbullying is treated as seriously as in-person bullying.

8.2. Prevention and response strategies are detailed in the School's Anti-Bullying Policy; this section should be read alongside that policy.

8.3. Online anonymity can embolden harmful behaviour. No one may use digital platforms to insult, threaten, harass, exclude, or spread rumours.

8.4. Expectations for respectful conduct apply online and offline. Intentional breaches will result in disciplinary action in line with school policies.

8.5. All reports of cyberbullying are taken seriously and investigated promptly. Where necessary, the School may review relevant systems, logs, and—subject to policy and law—school-managed or personally owned devices to establish the facts.

8.6. Incidents will be recorded and, where appropriate, referred to external agencies (e.g., the Police) at the discretion of the Executive Headmaster or designate.

8.7. The School will provide support and reassurance to the targeted individual and, where

appropriate, their family.

8.8. Those responsible for bullying will be clearly informed the behaviour is unacceptable and must stop immediately.

8.9. Where multiple individuals are involved, they may be spoken to both individually and as a group to determine roles, intent, and impact.

8.10. Pupils who have caused harm—physically or emotionally—will be supported to understand the impact of their actions and to make amends where appropriate.

8.11. Sanctions will align with the School's Behaviour Policies, and the rationale will be explained to those involved.

8.12. Individuals may be required to remove harmful or inappropriate content they have created or shared; if they cannot or will not, the School may contact the platform/service provider. Access to Capital School Bahrain IT services may be suspended while the matter is resolved.

9. Radicalisation

9.1. Radicalisation is the process by which individuals or groups adopt extremist beliefs - political, religious, or social - that may lead to intolerance, harm, or violence.

9.2. The School is committed to protecting pupils from extremist views and to developing critical thinking so learners can recognise, question, and resist attempts to radicalise them.

9.3. All members of the school community must promptly report any concerns or attempts to promote extremism or violent extremism - online or offline - to the Designated Safeguarding Lead or the Principal.

10. Use of Other Technology

10.1 **Removable media (USBs, SD cards, external drives):** Use responsibly and in line with the ICT Acceptable Use Policy. Do not connect removable media to the school network without explicit approval from IT. Where permitted, devices must be malware-scanned and (if holding sensitive data) encrypted.

10.2 **Headphones/earphones and personal electronics**: Must be off and out of sight during lessons unless a teacher explicitly authorises their use. Pupils' Mobile Phones must be left at home, or stored in Reception, for the duration of the school day. Owners are responsible for the security of personal items; the school accepts no liability for loss or theft.

10.3 **Security controls:** Bypassing filtering or other security measures is strictly prohibited and

risks both your device and the school network. Detected violations may result in your device being blocked from the network until cleared by IT. Repeated offences may lead to disciplinary action and suspension of access.

11. Education and Awareness

11.1. **Whole-community education:** Capital School Bahrain plays a central role in educating pupils, parents, and staff about online safety. Our programme covers technical and behavioural topics including grooming, radicalisation, age-inappropriate content, sharing personal information, digital footprints, cyberbullying, sexting, phishing and password hygiene, and responsible use of social media and digital communications.

11.2. **How it's delivered:** Online safety is taught across the curriculum (including ICT/Computing, PSHE, tutor time) and through assemblies and targeted sessions. Content is age-appropriate, revisited at key stages, and supported by staff CPD and parent information sessions.

11.3. **Access to the policy:** This policy is published internally and on the Capital School Bahrain website. Its key points are highlighted at least annually to pupils, staff, and parents to reinforce roles and responsibilities.

12. Disciplinary Procedures

12.1. Any breach of the aforementioned can and will result in disciplinary action.

12.2. Pupils and their parents/guardians are reminded that use of School Technology is a privilege and not a right and that everything done on any School-owned computer, network, or electronic communication device may be monitored by school authorities. Pupils who misuse the computer facilities and contravene the ICT Acceptable Use Policy will be subject to disciplinary procedures.

12.3. Any pupils found to be involved in recording, distributing or uploading inappropriate images or videos of pupils, parents or staff at any time will be suspended.