CBS
CREATIVE
BRITISH SCHOOL

BYOD/AUP Policy

Policy Created	September 2024
Policy Review date	August 2025

This policy has been adopted by the Creative British School Principal and board of Governors

Signed Principal: Mr.Phillip Morris

Date:01-09-24

مدرسة الإبداع البريطانية ذ.م.م
Abu Dhabi - U.A.E.
CREATIVE BRITISH SCHOOL L.L.C.

1. Rationale

In a world of consistently evolving technology, it is vital we prepare our children not only for the present but for the future also. The focus of this Acceptable Use Policy (AUP) / Bring Your Own Device (BYOD) policy is to provide resources, tools and protection to the 21st century learner. Excellence in education requires that technology is seamlessly integrated throughout the educational program. Increasing access to technology is essential for that future. The AUP/BYOD policy is a way to empower students to maximise their full potential and to prepare them for further education and the workplace.

Learning results will improve from the continuous dynamic interaction among students, educators, parents, and the extended community. Technology immersion does not diminish the vital role of the teacher. To the contrary, it transforms the teacher from a director of learning to a facilitator of learning. Effective teaching and learning with wireless technology tools integrate technology into the curriculum anytime, anyplace. The policies, procedures and information within this document apply to all wireless mobile devices used at Creative British School, including any other device considered by the Administration to come under this policy. Teachers may set additional requirements for use in their classroom.

2. Aims

At Creative British School, we aim to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain safe when using the internet and related technologies, in and beyond the context of the classroom.

In recognition of the increasing role of technology in education and the potential benefits of device usage for enhancing learning, this policy aims to establish guidelines and best practices for the responsible use of devices in educational settings. This policy aims to strike a balance between leveraging technology for educational enrichment and ensuring the well-being of students.

3. Definitions

Term	**CBS Definition**
Mobile Device	Any portable device that can be used for internet access, photography and/or video. Including but not limited to: laptops, desktop computers, tablets, iPads, mobile telephones and smart watches.
Social Media	Websites and applications that enable users to create and share content or to participate in social networking.

Fixed Device	Any school or home-based PC normally static in its location and connected to a network.
Filtered Internet	Whilst many unacceptable sites are blocked in the UAE, the school also applies its own layer of filtering to further protect students.
Firewall	Used to provide an extra layer of security to the school network and its users.

BYOD (Bring Your Own Device) includes all mobile devices and any wearable technology. BYOD, while not school property, also fall under the Acceptable Use Policy whilst on school property or whilst on school related activities.

However, the school is not responsible for the repairs, loss or theft or any damage resulting from their use on school property or during school related activities.

Improper use of BYOD will lead to immediate confiscation and permanent denied access to the school Wi-Fi network. The devices will only be returned to the parents or legal guardians of the student owning the device.

4 Internet Access

At Creative British School, the filtered internet is used as an educational development tool by staff and children. Staff have access to the internet for teaching and learning purposes only whilst on school site.

4.1 Managing the Internet

- Students will have supervised access to internet resources for educational purposes through the school's fixed and mobile technology. Students will access the internet whilst in school using personalised access codes.
- Staff will preview any recommended sites before use, in line with the Schools policies.
- If internet research is set for home learning, specific sites will be suggested that have been previously checked by the teacher. It is advised that parents also check and supervise sites which are used at home.
- All users must observe copyright at all times.

4.2 Internet Use

- You must not post personal, sensitive, confidential, or classified information or disseminate such information in any way that may compromise its intended use or audience.

- Names or personal details of colleagues, parents or children will not be acquired through any online mediums on school site. If students must sign up to educational sites, they will use their own school email, as appropriate.
- Online gaming, other than for educational purposes, will not permitted on school site.
- Internet activity can be monitored and explored further if required by a member of the Senior Leadership Team.
- If staff or pupils discover an unsuitable site or images, the screen must be switched off/closed and the incident reported immediately to a member of the Senior Leadership Team.
- Any adult or child caught viewing material that is not for educational purposes will be reported to a member of the Senior Leadership Team who will take any necessary actions.
- Our computing curriculum teaches children the importance of being 'Cyber Smart'.

5 Portable and Mobile Devices

At Creative British School, we use laptops and desk top machines for learning, teaching and assessment tools. Staff are responsible for the care and safe keeping of the devices belonging to the school. This includes the appropriate use and content saved on these devices.

- The school allows staff to bring in personal mobile phones and devices which may only be used during non-contact time or for emergency purposes.
- Under no circumstances does the school allow a member of staff to contact students or parents using their personal email or number.
- The sending of inappropriate messages or images between any members of the school community is not permitted, including staff, parents and students. A member of the Senior Leadership Team will be informed and deal with any matters in this incidence.
- Users bringing personal devices into school are responsible for ensuring that there is no inappropriate or illegal content.
- Pupils are not permitted to bring personal devices into school without the knowledge and permission of their teacher. Pupil mobile phones are not permitted in class and must be stored each morning at main reception.
- Parents are not permitted to take photographs of children other than their own on school site, without the permission of a teacher or member of the Senior Leadership Team.
- The school reserves the right to report the inappropriate use of mobile devices on the school site.

6 Screen time

This policy recognises the potential of screen time to enhance learning while emphasising responsible and purposeful integration. By adhering to these guidelines, we aim to harness the benefits of technology in education while safeguarding the well-being of our students.

Through collaboration among educators, parents, and students, we can create a balanced and effective learning environment that prepares students for success in the digital age.

Guidelines:

Purposeful Integration: screen time should be purposefully integrated into the curriculum to enhance learning outcomes. Educators are encouraged to identify specific learning objectives and activities that can be enriched through technology.

Age-appropriate Usage: the amount and complexity of screen time should be age-appropriate. Younger students may require shorter, more focused screen sessions, while older students can engage in more extended activities.

Quality Content: educational content on screens should be high-quality, evidence-based, and aligned with educational goals. CBS will regularly review and update the list of approved educational apps and websites.

Balanced Approach: a balanced approach to screen time is essential. It should complement, not replace, other forms of learning, such as face-to-face instruction, reading and hands-on activities.

Digital Responsibility Education: students should receive instruction on responsible digital behaviour including topics such as online etiquette, privacy and critical thinking skills to navigate the digital landscape effectively.

7 Social Media

At Creative British School, we use Twitter, Instagram and our school Facebook page as a platform to share and celebrate learning. When joining school, parents must sign to refuse permission for their child's photograph to be used on all forms of social media. A record of this is kept by the IT department and Registrar for online safety and shared with all staff. It is the responsibility of the members of staff to ensure that they adhere to this.

- Staff should ensure that their personal social media accounts have the highest privacy settings.
- No members of staff should share or friend students or parents on social media platforms.
- Any inappropriate posting on social media that affects the reputation of the school or staff will be reported to the Principal who will take the necessary action.
- Social media websites and applications will be blocked in school. Social media access is legally limited to those aged 13 and above. Parents are advised to adhere strictly to age restrictions.

8 Cyberbullying

8.1 Definition of Bullying

What is cyber bullying?

- Cyber bullying includes sending or posting harmful or upsetting text, images or messages using the internet, social media, phones or other digital technology.
- It can take many forms, but can go even further than face to face bullying by invading home and personal space and can target one or more people.
- It can include threats, intimidation, harassment, defamation, exclusion or peer rejecting, impersonation and unauthorised publication of private information or images.

Cyber bullying can be carried out in many ways, including:

- Threatening, intimidating or upsetting emails, text or images.
- Threatening or embarrassing pictures, video clips or text.
- Silent or abusive phone calls or using the victim's phone to harass others, making them think the victim is responsible.
- Unpleasant messages or responses.

In some cases, these types of bullying or defamation can be a criminal offense.

8.2 Prevention of Cyberbullying

At Creative British School, we have clear prevention strategies including:

- Dedicated members of staff oversee the practices and procedures outlined in this policy and monitor their effectiveness.
- Identification of signs of cyberbullying will be shared with staff through National Online Safety training.
- Pupils will be informed and taught about the risks and internet safety through our eSafety lessons, digital safety framework and pastoral activities.
- Child Protection training by dedicated members of staff will include cyber bullying identification and what to do.
- Positive use of digital technology will be promoted throughout the school and reviewed and monitored by the Digital Curriculum Leaders.
- Partnerships between home and school to encourage clear communication.

8.3 Digital Leader Framework

At Creative British School staff and students follow a Digital Leader Framework which runs community wide, this is also shared with parents to ensure the children are receiving the same information at home as they are at school. A network of digital leaders will be established throughout the school and children will work alongside staff to share eSafety and Cyberbullying messages with their peers.

This framework is built around the importance of a positive digital life and how we can prevent, educate and stop cyberbullying within our community.

8.4 Support

If an incident of cyberbullying is reported by a pupil, staff member or parent, it will be investigated by a member of the Pastoral Team. This will involve:

- Review of evidence and advice to preserve it, for example saving or printing of messages.
- Investigation to identify the perpetrator by looking at the media, sites and discussions with any witnesses.
- Requesting a pupil to reveal digital technology content. Staff do not have the authority to search the contents of a device.
- Reporting incidents of cyber bullying to the Vice Principal or Social Worker for eSafety who will take the necessary action in taking this further.

As with any form of bullying, support for the individuals will be dependent on the circumstances.

8.5 Regulatory References

Parents and students are reminded that in the UAE, there are extreme consequences for online defamation of character, person or organisations.

The Federal Law No. 5 2012 was issued by the President his Highness Sheikh Khalifa Bin Zayed Al Nayhan and is commonly known as the 'Cyber Crimes Law'. It is the Cyber Crimes Law that provides the most practical recourse for victims of crimes involving technology.

Article 20 deals with slander: any person who insults a third party or has attributed to him an incident that may make him subject to punishment or contempt by a third party by using an Information Network or an Information Technology Tool shall be punished by imprisonment and a fine not less than (AED 250,000) and not exceeding (AED 500,000) or by any of these punishments.

Article 16 of the Cyber Crimes Law states that a perpetrator of an action that could be considered to be extortion shall be punished by imprisonment for a period of two years at most and a fine not less than AED 250,000 and not in excess of AED 500,000, or either of these two penalties. Accordingly, threatening to bully someone unless money is received may lead to severe penalties – the act of bullying does not have to eventuate, it can simply be threatened. If the extortioner uses the threat of bullying (eg; "I'll tell everyone that you…") in order to extract money or something of value from the victim, they may be found guilty under this law.

Article 15 of the New Cyber Crimes Law also states that it is an offence for persons to intentionally and without permission capture and/or intercept communications online.

8.6 Monitoring, Roles and Responsibilities

Children and members of staff will report any incidents of cyberbullying to the appropriate member of the pastoral team. The member of staff will then:

- Investigate and gather the required information or evidence

- Discuss incidents with any or all of the students involved
- Meet with parents to feedback information and next steps in moving forward
- Use restorative justice principles and make any required referrals

9 Communication

All communication between members of our school community must be done so in a professional manner. The Principal/HR will speak directly with any members of staff, parents or children who do not adhere to this and any necessary action will be taken. Any matters of a sensitive nature should be communicated face to face during an arranged meeting time. Communication with parents will be via email and ClassDojo. Parents can email reception if they wish to contact a member of staff and are unable to come into school.

9.1 Email

- Staff can communicate with each other via their school email address.
- No staff members should email a child at any time.
- Any inappropriate emails should be reported directly to the SLT team.
- Confidential information regarding Creative British School should only be shared or emailed with authorised personnel.

9.2 Whatsapp

- CBS does not advocate the use of WhatsApp parent groups.
- WhatsApp will not be used as an official communication tool by CBS.
- Content related to other people's children should not be shared by parents on WhatsApp.

10 Roles and Responsibilities

10.1 Parent/Guardian Responsibilities

Parents have a responsibility to talk to their children about values and the standards that their children should follow regarding the use of the internet as they would in relation to the use of all media information sources such as television, mobiles, movies, podcasts, radio and social media. Additionally, parents are strongly encouraged to read communication and attend informative sessions provided by the school on the importance of e-Safety. We ask that parents support the school community in closely following guidelines for age restrictions on applications and social media websites.

10.2 School Responsibilities

- Provide Internet and Email access to its students.
- Provide Internet Blocking of inappropriate materials where possible.
- Provide data storage areas. These will be treated similarly to school lockers. The school reserves the right to review, monitors, and restrict information stored on

or transmitted via school owned equipment and BYOD devices and to investigate inappropriate use of resources.
- Provide staff guidance to aid students in doing research and help assure student compliance of the acceptable use policy.

10.3 Students Responsibilities

- Using computers/mobile devices in a responsible and ethical manner.
- Obeying general school rules concerning behaviour and communication that apply to technology equipment usage.
- Using all technology resources in an appropriate manner so as to not damage school equipment. This “damage” includes, but is not limited to, the loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by the students own negligence, errors or omissions. Use of any information obtained via the school’s designated Internet System is at your own risk. The school specifically denies any responsibility for the accuracy or quality of information obtained through its services.
- Helping the school protect our computer system/device by contacting an administrator about any security problems they may encounter.
- Monitoring all activity on their account(s).
- Students should always turn off and secure the mobile device and BYOD devices after they are done working to protect their work and information.
- If a student should receive communication containing inappropriate or abusive language or if the subject matter is questionable, he/she is asked to report it to a trusted adult.
- Returning the school mobile device to the class monitors at the end of each period/s or day.
- Ensuring all BYOD devices are fully charged at the start of the school day.
- Their BYOD device is brought to school each day unless otherwise informed.
- Ensure their BYOD device has the Apps/software installed as requested by the school and maintain software upgrades.

10.4 Student Activities Strictly Prohibited:

- Students must not take pictures or movies of students who have not given their permission to do so
- Any action that violates existing school policy or public law
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, religious or sexually explicit materials
- Use of chat rooms, sites selling exam papers, book reports and other forms of student work
- Internet/Computer Games without permission of the school.
- Changing of school mobile device settings (exceptions include personal settings such as font size, brightness, etc)
- Downloading apps at school unless supervised by the teacher and parental consent.
- Spamming-Sending mass or inappropriate communication

- Gaining access to other student's accounts, files, and/or data
- Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity
- Students are not allowed to give out personal information, for any reason, over the internet. This includes, but is not limited to, setting up internet accounts including those necessary for chat rooms, etc.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed.
- Bypassing the school web filter through a web proxy or VPN.

Mobile device and BYOD Care

- Students will be held responsible for maintaining their own devices and keeping them in good working order whilst in their possession.
- BYOD devices must be recharged and ready for school each day.
- The school will be responsible for repairing only school owned Mobile devices which malfunction. Mobile devices which have been damaged from student/staff misuse or neglect will be repaired with cost being borne by the student/staff. In the event of an accidental damage, the school on a case-to-case basis may exercise discretion in recovering the cost of repair to the device from the user.

Mobile device theft

- Mobile devices that are stolen must be reported immediately to School SLT/Principal and may require further reporting to the local police.
- The school is not liable for any loss of personal devices by either staff or children.