E-Safety Policy -Protecting Our Children

American Schools of Creative Science International Schools of Creative Science

Dubai and Sharjah

2021-2023

Excellence Rooted in Values and lighting the way for all means that the school has key values that all members of our school community live by. Underpinning our mission and vision are our guiding tenets of

Integrity Tolerance Collaboration Courage Compassion

These values apply to core life skills applicable to all stakeholders.

Lighting the way: Collectively, we pave the road to success to all our learners who strive to grow and nurture as they reach full maturity.

Excellence Rooted in Values: All of us, individually and collectively, work hard to ensure that our students develop a sense of purpose, character, transferability of skills, and assimilate the knowledge essential to become morally responsible global citizens. We not only foster academic excellence but also promote understanding of and respect for one another's beliefs and differences.

Policy Date	March 23, 2021
Policy endorsed by BEAM Governing Body	Shadi Hassan April 8, 2021
IT Approval Signature and Date	Mohamed Sadawy. March 23, 2021
Effective Date	April 11, 2021
Principal Approval Date	
Next Review Date	June 2022

Contents

1.The School E-Safety Policy Scope and Audience

The requirement to ensure that students can use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work with them are bound.

Digital technologies have become integral to the lives of students today. The Internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. It should be noted, however, that alongside this, there is a growing expression of opinion that unlimited use of mobile devices is not necessarily healthy for under 16-year-old children.

It is our vision that every learner has an entitlement to online learning and the use of appropriate learning technologies. Learners must have access to quality online learning opportunities in a variety of forms which meet their individual needs. In achieving this vision, students, staff, and other stakeholders always have a right to safer internet access.

We are committed to helping all members of the school community to benefit from information and communication technology, while understanding its risks, and to equipping students with the knowledge and skills to be able to use it safely and responsibly.

2.The E-Safety Policy Main Coverage

We believe that health and e-safety will be maintained only with the cooperation of all staff, students, and visitors to the school. We will ensure that all staff, students, visitors, and contractors are provided with the information they require to enable them to comply with this policy.

It is the intention of BEAM Governing Body and school leadership and management that procedures ensuring relevant health and safety issues are embedded within the curriculum at all levels where appropriate.

The effectiveness of the policy will be regularly monitored to ensure that health and e-safety arrangements are being implemented and that the people named in the policy are carrying out their duties. It is, therefore, important that all involved in delivering this policy maintain access to readily available evidence which supports good practice and so instils confidence in that practice. This E-Safety policy enables our school to create a safe e-learning environment that:

- Protects students from harm
- Safeguards staff in their contact with students and their own use of the internet
- Ensures the school fulfils its duty of care to students
- Provides clear expectations for all on acceptable use of the internet.
- Ensures the school’s technical infrastructure is secure and is not open to misuse or malicious attack

3. Policy Guiding Statements

Education of Students

While there remains an important emphasis to regulate use of technology within schools, this must also be balanced by educating students to adopt a responsible approach. As such the education of students in e-safety is an essential part of our schools’ e-safety provisions. Learners need guidance and support from the school itself to recognize and avoid online risks and to build their resilience as well as their ability to self-regulate.

To this end, E-safety shall be a focus in all areas of the curriculum and staff will work to reinforce e-safety messages across the curriculum. A broad, relevant curriculum will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of computing classes as well as personal, health, social and emotional wellbeing lessons

- Important, current e-safety messages should be reinforced as part of a planned program of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the material content they access online and be guided to validate the accuracy of information and respect copyright
- Students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet, and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material.
- Where students can freely search the internet, staff should be vigilant in monitoring the content of the websites they visit.

Education of Parents and the Community

The school recognizes that parents may have limited understanding of e-safety risks especially in relation to current trends. However, parents also play an important role in supporting their child's education and monitoring and regulating their online behavior and habits. Parents may not be aware of the potential or under-estimate the risk of their child coming across potentially harmful or inappropriate content whilst online. In addition, parents may not be sure how to respond to inappropriate use of the internet.

The school will support parents by:

- Holding parent workshop sessions
- Publishing letters, newsletters
- Holding high profile events such as Safer Internet Day
- Providing family learning courses in use of new digital technologies, digital literacy, and e-safety
- Updating the school website to provide e-safety content for the wider public

Education of Staff and Governors

Staff will receive e-safety training to support their understanding of their responsibilities as outlined in the policy. Training will be offered to equip staff to fulfill their roles and responsibilities as follows:

- A program of formal e-safety training will be made available to staff, which will be regularly updated.
- An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process
- All new staff should receive e-safety training as part of their induction program, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements
- The E-Safety Coordinator will receive regular updates through attendance at external training events

4. Information Security And Maintenance

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and learners.

The network and security issues include:

- Users must act reasonably — e.g. downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For school staff, breaching electronic use policy is regarded as a reason for dismissal.
- Staffrooms/Workspaces should be secured against user mistakes and deliberate actions.

- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date; through regular monthly patching
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured.
- School broadband firewalls must be configured to prevent unauthorized access between schools.
- School broadband network must be protected by a cluster of high-performance firewalls at the Internet connecting nodes.

School action points to secure measures:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used unless it has been encrypted and virus checked.
- Unapproved software will not be allowed in school or attached to email.
- Files held on the network will be regularly scanned.
- System capacity in relation to storage will be monitored regularly.
- The use of user logins and passwords to access the network will be enforced.

Managing Access & Content Filter Management

All Creative Science students and users have an account on MS Office 365. All users must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.

- The school's broadband access provides filtering appropriate to the age and maturity of learners. There is flexibility in the filtering system to allow for changes in provision depending on the learning required.
- A description of the content filtering service is shared with the school (Infrastructure).
- School has its own tenancy, allowing or blocking URLs or full categories as required.
- The school blocks access to social networking sites.
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are asked to report any incidents of cyberbullying to the school.
- School staff are advised not to add students, or parents as 'friends' if they use unauthorized sites.
- Students must not send or attach documents containing offensive, threatening, derogatory, racist, or sexually explicit material.
- If any of the above is received by a user, a staff member must be informed.
- Students must not harass other users. This includes forwarding chain letters; deliberately flooding a user's mailbox; sending mail that is designed to interfere with the e-mail system.
- Students must not access, copy, or transmit another student's message or e-mail address without their permission.
- Students must not forge a message to make it appear to come from another person.
- If staff or learners discover unsuitable sites, the URL will be reported to the Data and risk-assessment manager who will then record the incident and escalate the concern as appropriate.
- The School content filtering system will block all sites on the Internet that contradict ethos and values.
- Changes to the school content filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will affirm that regular checks are made to ensure that the filtering methods selected are effective.

- Any material that the school believes is illegal will be reported to appropriate authority.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the learners, with advice from network managers.

5. E-Safety Monitoring Process

As a school, it is a vital duty of care alongside that of parents and other members of the community to protect students and this can be achieved by many different mechanisms working together. The e-safety policy will be actively monitored and evaluated by an e-safety committee. This committee will comprise:

- E-safety Coordinator/Officer
- Principal
- Designated Safeguarding Lead(s)
- Teaching Staff (1 in each phase)
- Internal IT personnel
- External IT contractors

In the event of an e-safety incident, the following people will be informed within school

- School E-Safety Coordinator
- Principal
- Designated Safeguarding Lead(s)

6. E-Safety And School Leadership & Management

School senior leadership team is responsible for determining, evaluating and reviewing e-safety policies to encompass teaching and learning, use of school IT equipment and facilities by students and visitors, and the agreed criteria for acceptable use by students and school staff.

The e-safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with stakeholders and outside organizations; technological and Internet developments, current government guidance and school related e-safety incidents.

The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine provision for staff and guidance provided to parents, students, and local partnerships.

E-safety provision is always designed to encourage positive behaviors and practical real-world strategies for all members of the school and wider school community.

The leadership team is encouraged to be aspirational and innovative in developing strategies for e-safety provision.

7. The School E-Safety Coordinator Roles And Responsibilities

The E-Safety Coordinator's responsibilities are outlined as follows:

- Leads the e-safety committee
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place

- Ensures the school's e-safety committee meets regularly and has conquering meetings.
- Responsible for e-safety issues on a day to day basis and liaises with filtering and website providers and school ICT support.
- Audits and assesses system requirements for staff, support staff and e-safety training, and ensures that all staff are aware of their responsibilities and the school's e-safety procedures.
- Provides training and advice for staff
- Promotes best practice in e-safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.
- Receives reports of e-safety incidents and maintains a log of e-safety reports and incidents to inform future e-safety developments and inform training needs or education updates required
- Meets regularly with Safeguarding Governor to discuss current issues, review incident logs relevant meeting
- Along with IT support, is involved in any risk assessment of new technologies, services, or software to analyze any potential risks
- Takes part in strategy discussions and inter-agency meetings and/or support other staff to do so.
- Provides advice and support to other staff on child welfare and child protection matters.
- Follows any instructions or guidelines for the Distance Learning Initiative issued by the Ministry of Education/KHDA/Regulatory Authority
- Reports regularly to Senior Leadership Team

The school has a designated e-safety Coordinator who reports to the SLT and coordinates e-safety provision across the school and wider community. The e-safety committee liaises with SLT, the schools designated safeguarding leads and other senior leaders as required.

The school's e-safety coordinator chairs the e-safety committee which includes representatives of the SLT, teaching and support staff.

The coordinator is also the first point of contact for staff requiring advice on e-safety matters. Although all staff are responsible for upholding the school e-safety policy and safer Internet practice, the e-safety Coordinator, the principal, heads of phases and ICT support are responsible for monitoring Internet usage by students and staff.

8. ICT Support Staff And External Contractors

External ICT support staff and technicians are responsible for maintaining the school's networking, IT infrastructure and hardware. They are aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure. They further ensure that systems are not open to abuse or unauthorized external access.

Support staff maintain and enforce the school's password policy.

External contractors, website designers/hosts/maintenance contractors are made fully aware of and agree to the school's e-safety Policy. Where contractors have access to sensitive school information and material covered by the data protection, school website or email provision.

School ICT support staff is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required e-safety technical requirements
- Support staff keeps up to date with e-safety technical information to effectively carry out their e-safety role and to inform and update others as relevant

- The school meets required e-safety technical requirements and any regulatory authority E-Safety Policy / Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The content filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Procedures are in place to follow up on usage reports for teachers and students and to develop a plan to improve performance and quality of use.
- The school follows any instructions or guidelines for the Distance Learning Initiative issued by the Ministry of Education/any regulatory authority.
- The school keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- Monitoring the use of the network/internet/Virtual Learning Environment/remote access/email is evident so that any misuse can be reported to the Head of Section/Principal/Senior Leaders/E-Safety Coordinator

9. Teaching And Teaching Support Staff

Teaching and teaching support staff need to ensure that they are aware of the current school e-safety policy, practices, and associated procedures for reporting e-safety incidents. They will be provided with e-safety induction as part of the overall staff induction procedures.

All are responsible to ensure that

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood, and signed the Acceptable Use Policy relevant to Internet and computer use in school.
- They follow the school's social media policy, regarding external off-site use, personal use (mindful of not bringing the school into disrespect), possible contractual obligations, and conduct on Internet school messaging or communication platforms, for example email, messages and the school website.
- They report any suspected misuse or problem to Head of Section for investigation
- All digital communications with students and parents are professional and carried out only using official school systems
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies regarding these devices
- They are aware of online propaganda and help learners with critical evaluation of online materials.
- The Internet usage and suggested websites are pre-vetted and documented in lesson planning.

10. Social Workers And Support Staff

Social workers and support staff are responsible for ensuring that:

- They promote awareness on all forms of bullying for students, parents, and staff members.
- They run national anti-bullying week program.
- They maintain and review the school's Anti-bullying and Cyberbullying policy
- They bring cases to behavior management committee/ E-safety committee.

- They follow the school Anti-bullying policy and MOE behavior policy when dealing with e-safety cases.
- They maintain records of all cases reported and secure.

11. Staff Use Of Personal Devices

Staff are responsible to follow the guidelines as set below:

- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity, then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of learners and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

12. Students' Use Of Bring Your Own Devices

All students are required to follow the guidelines as set out in the school's BYOD Policy.

Phones and devices must not be taken into examinations. Learners found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

If a learner needs to contact his/her parents, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

13. Designated Safeguarding Leads

The Designated Safeguarding Lead is trained in specific e-safety issues and is aware of potential serious child protection issues that can arise from the following:

- Allegations against members of staff
- Computer crime – for example, hacking of school systems
- Sharing of personal data
- Access to illegal or inappropriate material
- Inappropriate online contact with adults/strangers
- Allegations or evidence of 'grooming'
- Allegations or evidence of Cyberbullying in the form of threats of violence, harassment, or a malicious communication.
- Producing and sharing of youth produced sexual imagery.

The Designated Safeguarding Lead can differentiate which e-safety incidents are required to be reported to BEAM Safeguarding Governors, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

14. Students

- Are required to use school Internet and computer systems in agreement with the terms specified in the school's Acceptable Use Policy. Students are expected to sign the policy to indicate agreement, and/or have their parents sign on their behalf.
- Know and understand policies on the taking / use of images and on cyber-bullying
- Need to be aware of how to report e-safety incidents in school, and how to use external reporting facilities.
- Need to be aware that the school's Acceptable Use Policies covers all computer, Internet, and mobile technology usage in school.
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and need to be aware that their Internet use out of school on social networking sites such as Facebook, Instagram is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and students in terms of cyber bullying, reputation, or illegal activities.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

15. Parents and Guardians

The school recognizes that Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school is committed to taking every opportunity to help parents understand these issues through parents' evenings, newsletters, website, and information about local e-safety campaigns. Parents will be encouraged to support the school in promoting good e-safety practice and following guidelines as set out in relevant policies related to online use and behavior.

Parents are responsible for ensuring that:

- Children are monitored when they are online, especially during online learning phase.
- They are warned of the negative side of communication technology.
- Children are instructed to report any concerns to them or the school management.
- They help their child act with self-confidence.
- They support the school's stance on promoting good Internet behavior and responsible use of IT equipment and mobile technologies both at school and at home.
- They sign the school's Acceptable Use Agreement, indicating agreement regarding their child's use and their own use regarding parental access to school systems such as iCampus, websites, social media, online reporting arrangement, and surveys.

(Refer to Wellbeing Policy, refer to the BYOD, Acceptable Use Policy, E-Behavior Management Policy, Safeguarding and Child Protection Policy)

16. Provisions For E-Safety Education

The Curriculum Leader

- Support e-safety policies by ensuring that e-safety is taught effectively within the curriculum for all year groups.
- Support the e-Safety Coordinator in developing educational materials for students which can be delivered outside of the curriculum.

Throughout the curriculum, teaching about potential harms will include many of the following as applicable:

- Age restrictions
- Content: How it can be used from credible sources
- Disinformation, misinformation, and hoaxes
- Fraud (online) and Fake websites and scam emails
- Password phishing and Personal data
- Persuasive design which keeps 'users online for longer than they might have planned or desired'
- Privacy settings, Targeting of online content, and Abuse (online)
- Challenges [to do something and post about it]
- Content which incites…hate, violence
- Fake profiles and Grooming
- Live streaming and Pornography
- Unsafe communication
- Impact on quality of life, physical and mental health, and relationships
- Online vs. offline behaviors
- Reputational damage

(Refer to Technology Classroom Integration Policy and Plan)

17. Personal Information On The School Website

No material defined as ‘personal information’ will be used on the school website without the consent of persons concerned.

The School considers staff privacy issues carefully when publishing staff email addresses, staff lists, photos of staff, staff qualifications and any other personally identifying information.

18. Unsuitable / Inappropriate Activities - Acceptable Use

The school believes that the activities that contradicts and act against moral and ethical behavior, including any violation in any of the areas mentioned under this policy would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. Additionally, the use of these new and rapidly developing technologies can put users at risk as below

- Access to illegal, harmful, or inappropriate images or other content
- Loss of privacy / control of personal information
- Grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyberbullying

- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy, and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Hacking, viruses, and system security
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

19. UAE Legislation and School Supporting Policies

- UAE Law Safeguarding Rights of Children 2017
- UAE Federal Law No.3 2016 Article 3 on Child Rights (Wadeema's law).
- NEASC/CIE Child Protection Standards of 2015
- UK Act on Keeping Children Safe in Education of 2015
- The United Nations Convention on the Rights of the Child (UNCRC): articles 3,12,19, & 36
- Federal Law No. 5 of 2012 on Combatting Cybercrimes & Cyberbullying Policy
- Telecommunications Regulatory Authority
- UAE Internet Access Management (IAM)
- UAE laws and resolutions concerning activities conducted online.
- Federal Law No. 7 of 2002 on Copyrights and related rights
- Federal Law No. 17 of 2002 on Regulation and Protection of Industrial Property of Patents, Industrial Drawings (Arabic)
- Ministerial Resolution No. 11 of 1993 on Executive Regulation of Law No. 44 of 1992 on Regulation and Protection of Industrial Property of Patents, Drawings and Designs (Arabic)
- Federal Law No. 37 of 1992 on Trademarks) Arabic)
- Dubai Data law: data protection and privacy of the individual.

School Supporting Policies

- Bukhatir Acceptable use policy
- Bukhatir Data Classification Policy
- Bukhatir Data Protection Policy
- BYOD Acceptable use policy
- Acceptable use policy for staff, visitors, and volunteers
- Safeguarding and Child Protection
- Consent form for parents and carers (including use of images)
- Personal data policy
- Guidance for reviewing internet sites (for suspected harassment and distress)
- Reporting log and Monitoring log
- Password security policy
- Beam password construction guidelines
- Wellbeing & Behavior Management Policy