E-Safety Policy

‘Your Digital Footprint Matters’

2024-2026

Policy Date	March 23, 2021	**Effective Date**	April 8, 2021
Policy endorsed by BEAM Governing Body	Shadi Hassan		
Chair of Governors			
Principal			
Last Review	August 2024		
Next Review Date	June 2026		

Contents

Introduction **3**

Background/Rationale **3**

Purpose **4**

Scope **4**

Roles and Responsibilities **4**

Teaching and Learning **4**

World Wide Web **5**

Social Networking **5**

Mobile Phones **6**

Digital/Video Cameras **6**

School Website **6**

Information System Security **6**

Assessing Risks **6**

Prevent Statement **6**

Cyber Bullying **7**

Handling E-Safety Complaints **7**

Communication of Policy **7**

Introduction

BEAM Creative Science Schools prioritize the safety and welfare of students, ensuring they can safely access technology and participate in the digital world. E-safety encompasses safe internet use and technology application.

Background/Rationale

New technologies are integral to children's lives, enhancing learning opportunities. Children have the right to safe internet access, which is part of the school's duty of care. This policy aims to ensure safe and appropriate technology use, involving all stakeholders in a child's education.

The internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should always have an entitlement to safe internet access.

The requirement to ensure that children and young people 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 in BEAM schools are bound. This school e-safety policy should help to ensure safe and appropriate use.

The development and implementation of such a strategy should involve all the stakeholders in a child's education from the principal and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorized access to / loss of / sharing of personal information
- The risk of being subject to 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
- Cyber-bullying
- 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
- The potential for excessive use may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviors, anti-bullying and safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Purpose

The E-Safety policy aims to create a safe e-learning environment that:

- Protects children from harm.
- Safeguards staff interactions with students.
- Fulfills the school's duty of care.
- Sets clear expectations for internet use.
- Protect and educate students and staff on technology use.
- Inform teachers and parents about safeguarding roles.
- Prevent and manage cyber-bullying incidents.

Scope

This policy applies to all members of the school community with access to ICT systems, both in and out of school.

Roles and Responsibilities

- **Governors:** Approve and review the E-Safety Policy.
- **Principal/Senior Leaders:** Ensure safety and delegate responsibilities to the computing coordinator.
- **Computing Coordinators:** Manage e-safety issues, provide training, and log incidents.
- **Staff:** Stay updated on e-safety, report issues, and embed e-safety in the curriculum.
- **Students:** Follow the Acceptable Use Policy and report misuse.
- **Parents/Carers:** Support children in using the internet responsibly.

Teaching and Learning

The school recognizes the internet as an essential element for education, business, and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and students. Therefore, the school has a duty to provide students with quality internet access as part of their learning experience. By providing a safe and structured internet environment, the school aims to equip students with the necessary skills and knowledge to navigate the online world effectively and responsibly.

- Internet access is essential for education, with appropriate content filtering.
- Students will be educated on acceptable internet use and digital literacy.
- Teachers will ensure websites used for assignments are appropriate.
- The school's internet access will be designed expressly for students' use, including appropriate content filtering.
- Students will primarily use a safe domain to access the computing curriculum.

- Students will be given clear objectives for internet use and taught what constitutes acceptable and unacceptable use.
- Students will be educated in the effective use of the internet for research, including skills such as knowledge location, retrieval, and evaluation.
- As part of the Computing curriculum, all year groups have digital literacy units that focus on different elements of online safety. These units cover topics like using search engines, understanding digital footprints, and preventing cyberbullying.
- When children are directed to websites as part of home learning, the teacher setting the learning will have checked them for appropriateness.

World Wide Web

The internet opens new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or students encounter unsuitable content online, they should immediately report the URL, time, and nature of the content to a teacher. The teacher will then log the incident in the e-safety record. The e-safety coordinator will review these logs on a termly basis.
- Students will be taught to be critically aware of the materials they are shown and how to validate information before accepting it accuracy.
- The school will work with its technical support provider to ensure filtering systems are effective as possible. Schools will have in place web-filtering that blocks access to social media sites, chat rooms, online gaming sites and certain video hosting websites that do not have an internal filtering system.

Social Networking

Social networking sites facilitate online chatting and information exchange, creating a digital environment that differs significantly from face-to-face interactions, often leading to behaviors that may not occur in person.

- Use of social networking sites is prohibited within the school and will be blocked or filtered.
- Students are advised against sharing personal details that could identify themselves, other students, their school, or their location, including personal photographs and videos.
- Parents and students will be informed that social networking use is inappropriate for primary-aged children outside of school.
- Students should only interact with known friends, family, and staff online, denying access to others.
- Staff are advised not to connect with parents or children on social networking platforms.
- Parents, students, and staff will be made aware of the risks associated with discussing students, staff, or the school on social networking sites. The governing body may consider legal action to protect against cyberbullying and defamatory comments.
- For any queries regarding this policy, please refer to the social media policy.

Mobile Phones

- Mobile phones are not allowed but must be handed to school administration during school hours.
- Staff must use school phones to contact parents.

Digital/Video Cameras

- Students may not use cameras without authorization.
- Staff must educate students on the risks of sharing images online.
- Consent is required before publishing student images.

School Website

- The school website provides essential information for parents and prospective parents.
- Contact details include the school address, email, telephone, and other numbers.
- Personal information about staff and students will not be published.
- The Principal and Vice Principal(s) will oversee content accuracy and appropriateness.
- Photographs and videos featuring students will be carefully selected to avoid individual identification.
- Students' full names will not be associated with any images on the website.
- Parental consent will be obtained before publishing Students photographs.
- Parents may share images of their children on social media but must seek permission for images including other children.
- The governing body may prohibit photography by parents who do not adhere to school policy.

Information System Security

- Regular reviews of school ICT systems' capacity and security will be conducted.
- Virus protection will be installed and updated frequently.
- E-safety discussions will be incorporated into agreements with the governing body.

Assessing Risks

- The school will take reasonable precautions to prevent access to inappropriate material, though complete elimination of risks is not guaranteed.
- Regular audits of ICT use will assess the adequacy of the e-safety policy and its implementation.

Prevent Statement

- The school complies with all UAE guidance to prevent individuals from being drawn into wrong doings.
- The focus is on keeping students safe from radicalization and extremism.

- Filtering systems will block inappropriate and extremist content; any unlocked content must be reported.

Cyber Bullying

Online bullying via messaging, texting, and chat rooms poses serious risks to students. Strategies to prevent online bullying are outlined in the policy, including:

- Prohibiting access to mobile phones and public chat rooms.
- Teaching students about safe internet use and providing resources.
- Encouraging students to report concerns about online bullying.
- Addressing complaints in accordance with the Anti-bullying Policy.

Handling E-Safety Complaints

- Internal internet misuse complaints will be addressed by the principal.
- Staff misuse complaints must be referred to the principal.
- Safeguarding and Child protection complaints will follow school procedures.
- The complaints procedure will be communicated to students and parents.

Communication of Policy

Principal and Senior Leaders

- The Principal and Vice Principal are responsible for ensuring the safety (including e-safety) of members of the school community, through the day-to-day responsibility for e-safety will be delegated to the e-safety officer.
- The Principal/Senior Leaders are responsible for ensuring that the e-safety officer and other relevant staff receive suitable CPD training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Principal/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the e-safety officer.
- The Principal/Senior Leaders should be aware of the procedures to be followed in the event of a serious e- safety allegation being made against a member of staff.

Students and the E-Safety Policy

- Rules for internet access will be displayed in all networked rooms.
- Students will be informed that their internet use is monitored.
- In Key Stage 2 (Grades 3-6), students will learn about the importance of safety on social networking sites, reinforced in computing lessons across all year groups.

Staff and the E-Safety Policy

- All staff will receive the school e-safety policy, with its importance explained.
- Staff must be aware that internet traffic can be monitored and traced; discretion and professionalism are essential.

Parents and the E-Safety Policy

- Parents will be directed to the school e-safety policy on the website.
- Regular updates on e-safety will be provided through leaflets and emails.
- Parents are encouraged to discuss the code of conduct with their children before signing the 'Student Acceptable Use Policy.'

Designated Safeguarding Leads

The Designated Safeguarding Leads (DSLs) should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

e-Safety Coordinator

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff
- Liaise with school's ICT technical staff
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.
- Meets with the principal to discuss current issues and review incident logs
- Attending relevant meetings.

This policy aims to foster a safe digital environment for all members of the school community. It will be reviewed bio-annually.