

E-Safety Policy



The British Muslim School

You are the best nation raised up for humankind. You enjoin righteousness, forbid corruption and you believe in Allah. Al- Quran, Surah Al-Imran, ayah 110

Title	E-Safety Policy
Document Type	Approved
Subject	E-Safety
Created	September 2024
Approved by	Board of Governors
Review Date	September 2025 or earlier where there is a change in the applicable law affecting this Policy Guidance
Responsible person:	Principal/DSL/Governing body

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable. "From: Safeguarding Children in a Digital World. BECTA 2006

The Department for Education published the revised statutory guidance 'Keeping Children Safe in Education' (KCSIE) in September 2023 for schools and colleges in England. Among the revisions, schools are obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Schools in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology".

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy operates in conjunction with other policies including those for Child Protection and Safeguarding, Discipline and Behavior Policy, Anti-Bullying, Code of Conduct for Staff, Acceptable Use policy, Curriculum and Confidentiality.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems

1.0 School e-safety policy

Writing and reviewing the e-safety policy

- Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors.
- It is shared with parents via the school website which also provides links to further information on e-safety.
- E-Safety issues are included in the Child Protection and safeguarding, Acceptable Use, Health and Safety, Anti- Bullying, PSHCEE and ICT policies.

2.0 Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

Internet use will enhance learning

- The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content and stay safe when using the internet, social media and electronic devices

- If staff or students discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT Coordinator.
- Staff should ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school provides e-safety training for students through ICT, assemblies, PSHCEE and other subjects

3.0 Managing Internet Access

- Information system security
 - The security of the school information systems will be reviewed regularly.
 - Virus protection will be installed and updated regularly.
 - The school uses broadband with its firewall and filters.

E-mail

- Students may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- Students must immediately tell a teacher if they receive offensive-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or student's personal information will not be published.
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.
- Students' work can only be published with the permission of the student and parents.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Students are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

4.0 Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or students discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden and will be treated very seriously.
- Staff have access to a school phone where contact with students is required. Otherwise, they may only use their mobile phones in the staff room.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998, amended in 2003. Refer to our Data protection policy for further detail.

5.0 Policy Decisions

Authorising Internet access

- The school will maintain a current record of all staff and students who are granted Internet access.
- Parents and students will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The principal will ensure that the e-Safety Policy is implemented and compliance with the policy is monitored regularly.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaint's procedure.
- Sanctions within the school discipline policy include:
 - interview/counselling by class teacher /principal;
 - informing parents or carers;
 - removal of Internet or computer access for a period.
 -

6.0 Communications Policy

Introducing the e-safety policy to students

- Rules for Internet access will be posted in all networked rooms.
- Students will be informed that Internet use will be monitored.
- Training in e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.
- Students will be informed they can report any concern they have to the teacher in charge who will treat this as a safeguarding risk, and therefore take prompt action to report matters to the DSL and principal.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- The school will provide e-safety training for all staff, as part of our safeguarding procedures.
-

Parents and the e-safety policy

- It is widely recognized that children are more likely to be incited to engage in risky behavior and drawn into extremist views and terrorist activities out of the school gates than while in school. For this reason, the school will endeavor to engage parents in e-safety education.
- The school will provide up to date advice to parents on various aspects of e-safety to help them safeguard their children at home; this advice will be communicated via the website, newsletters and meetings
- In addition, the school will invite parents to face-to-face training where and when appropriate

Criminal law

The school is fully aware that some types of harassing or threatening behavior – or communications – could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, the Public Order Act 1986 and the Counter Terrorism and Security Act 2015, with the associated Prevent Duty 2015.

Monitoring and evaluation of this policy

- Every member of staff is responsible for close supervision of use of the internet and electronic devices by students.
- The SLT members are responsible for ensuring that every member of staff and student makes appropriate use of the internet and electronic devices.
- The ICT coordinator is responsible for carrying out weekly checks to verify that this policy is implemented properly and for responding to concerns from staff, students or parents.
- The DSL is responsible for checking that the ICT coordinator, students and staff implement this policy and that no security breach occurs.
- The proprietors are responsible for ensuring that all who work at the school are properly safeguarded at all times. They should ensure that this policy is implemented consistently as part of their annual safeguarding audit.
- The views of staff, students and parents will be taken into consideration in the annual evaluation of this policy by the SLT.

