

E-Safety Policy

Introduction

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up 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.

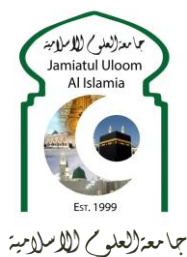
Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

This e-safety policy will help to ensure safe and appropriate use. The use of these 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.
- Unauthorised access to, loss of or 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 which 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 read and used in conjunction with other school policies; specifically, Anti-Bullying, Behaviour, Child Protection and Mobile Phone Use.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students'



جامعة العلوم الإسلامية
Jamiatul Uloom
Al Islamia
Est. 1999

Jamiatul Uloom Al Islamia
High School for Boys
Empowering today's youth for tomorrow

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 provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body, Mr Mohammed Miah, has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Meetings with the ICT and E-Safety Coordinators
- Regular monitoring of e-safety incidents
- Monitoring of filtering
- Reporting to relevant Governors and/or committee(s) meetings.

Headteacher & Senior Leadership Team (SLT)

The Headteacher is responsible for ensuring:

- The safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the Designated Safeguarding Lead (DSL)
- Adequate training is provided
- Effective monitoring systems are set up

- That relevant procedure in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school e-safety policies and documents
- The school's Designated Child Protection Officers should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.
- Liaising with staff, E-Safety Governor and SLT on all issues related to e-safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Providing training and advice for staff;
- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- Co-ordinating and reviewing e-safety education programme in school

ICT Coordinator

The ICT Coordinator is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements
- The school's password rules is adhered to
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Co-ordinator keeps up to date with e-safety technical information
- The use of the school's ICT infrastructure (network, remote access, e-mail etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the DSL and/or SLT for investigation/action/sanction.
- Must remove access from members of staff who have been suspended or have left the school

Teaching and Support Staff

All teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school's e-safety and acceptable usage policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Students (to an age appropriate level)

- Are responsible for using the school ICT systems in accordance with the Student Usage Policy.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues.

Community Users

Community Users who access school ICT systems/website will have restricted access. All activity will be logged and monitored.

Education and Training

E-safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of the form tutor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are helped to understand the need and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices
- Specific computing lessons are dedicated to teaching about online safety. These lessons are adapted to be age and developmentally appropriate to cater for all age groups.
- Students are taught about acceptable and unacceptable online behaviour and how to identify possible online risks and make informed decisions about how to act.

- Students are given guidance on how and when to seek support if they have been affected by something they have seen online.
- All staff and students will receive up-to-date training on the safe and effective use of emerging digital platforms.

Copyright

- Students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / children should open the selected image and go to it's website to check for copyright.

Staff Training

- E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- A planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Child Protection Policies.
- The **E-Safety Coordinator/SLT link** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- **Governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Communication

Email

- Digital communications with students (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems.

Mobile Phones

- **School** mobile phones only should be used to contact parents/carers, or students when on school business with students off site. Staff should not use personal mobile devices.
- **Staff** may only use personal mobile phones in school during working hours when in contact with children for school related activities in an emergency.

- Students should not use personal mobile phones in school during school hours.
- All mobile phones are to be handed into the school office at the start of school, then collected again at the end of the school day.
- Student mobile phones must not have a digital camera or have smart functionalities.

Social Networking Sites

Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on school equipment in school or at home. Staff should access sites using personal equipment.
- **Staff** users should not reveal names of staff, students, parents/carers or any other member of the school community on any social networking site or blog.
- **Students/Parents/carers** should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.
- Students in the KS3 & KS4 curriculum will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Digital Images

Please refer to Digital Recording Policy

Removable Data Storage Devices

- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks.
- Students should not bring their own removable data storage devices into school unless asked to do so by a member of staff
- Any data stored on removable data storage devices containing sensitive information related to the school should be encrypted so that the data cannot be accessed if it is lost or stolen.

Websites

- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use.

- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research.
- **All** users must observe copyright of materials published on the Internet.
- Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at school is tracked and logged.
- The school only allows the DSL, ICT co-ordinator and SLT to access to Internet logs.

Remote education

It is important for parents and guardians to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school their child is going to be interacting with online.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- We encourage passwords to be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Students

- Should only let school staff know their in-school passwords.
- Inform staff immediately if passwords are traced or forgotten. ICT lead teacher(s) are able to access the network to allow students to change passwords

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher or ICT co-ordinator.
- Students should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment;

- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

Use of the school's Internet access may be logged and the logs can be randomly but regularly monitored by the school's external provider. Whenever any inappropriate use is detected it will be followed up by the DSL or members of the Senior Leadership Team depending on the severity of the incident.

- The DSL and ICT Co-ordinator will maintain the Control Log and record any breaches, suspected or actual, of the filtering systems
- Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the DSL and impounds the equipment. This is part of the school safeguarding protocol. (If the concern involves the DSL then the member of staff should report the issue to the Principal).

Incident Reporting

Any e-safety incidents must immediately be reported to the Headteacher (if a member of staff) or the DSL (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

Responding to incidents of misuse

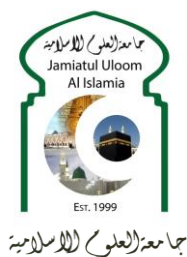
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed below in the tables are the acceptable/unacceptable activities and its responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will

be dealt with through normal behaviour/disciplinary procedures as follows (Appendix 1 for students and Appendix 2 for staff respectively).

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or				✓	



جامعة العلوم الإسلامية

Jamiatul Uloom Al Islamia

High School for Boys

Empowering today's youth for tomorrow

other safeguards employed by BMBC and / or the school					
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non-educational)		✓			
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites				✓	
Downloading video broadcasting e.g. Youtube		✓			
Uploading to video broadcast e.g. Youtube				✓	

364-370 Leagrave Road,
Luton, Beds, LU3 1RF
Tel: 01582 595535
DfE No: 821/6006
Charity No: 1084269
www.jamialuton.org
info@jamialuton.org



Appendix 1

Incident involving students	Teacher to use school behaviour policy to deal with	Refer to ICT Coordinator	Refer to police	Refer to technical support staff for action re security/filtering etc
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device.	✓			
Unauthorised use of social networking/ instant messaging/ personal email	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive,		✓		✓

harassment or of a bullying nature				
Continued infringements of the above, following previous warnings or sanctions		✓	Community Police Officer referral	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

The guidance in this policy should be implemented with cross reference to the schools Safeguarding, Anti-Bullying and Behaviour Policies. Note, attempts have been made to synchronise guidance and sanctions.

Appendix 2

Incidents involving members of staff	Refer to the Principal *See below	Refer to technical support staff for action re filtering, security etc	Referral to LBC specialists Potential Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓
Deliberate actions to breach data protection or	✓	✓	✓

network security rules			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ students	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓

***In event of breaches of policy by the Principal, refer to the Chair of Governors.**

Date of last review: March 2025

Date of next review: March 2026

Review period: 1 years