ONLINE SAFETY POLICY

THE ETHOS OF IQRA ACADEMY

IQRA means 'Read'

Improvement
Quality
Respect
Achievement

Policy Statement

New technologies have become integral to the lives of children and young people in today's society, both outside and within school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, improve literacy and communication skills, 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.

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

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- Inappropriate communication/contact with others, including strangers
- Online bullying
- Access to unsuitable video/Internet games
- Potential for excessive use which may impact upon the social and emotional development and learning of the young person
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- The risk of being subject to grooming by those with whom they make contact on the Internet
- Being exposed to extremist material promoting terrorism

As with all of these risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision to build pupils' awareness to the risks which they may be exposed, so that they have the confidence and understanding to seek advice and to deal with any risks in an appropriate manner.
This policy aims to create a secure and safe environment which develops technology skills and provides pupils with awareness of potential online Safeguarding scenarios that may arise.

The Online Safeguarding Committee

Mrs S Anwar-Bleem – Principal, Designated Safeguarding Lead
Mrs R Naylor - Computing Coordinator
Mr M Y Hussain - Named Governor for Child Protection
Mr R Aziz – Named Governor for Online Safety
Mr Z Nafees – Learning Leader
Pupils from the across the school council

The committee meets fortnightly to discuss safe guarding issues and monthly with school council to discuss pupils' views and opinions.

Internet Use Will Enhance Learning

- The academy Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported Online Safety incidents
- Monitoring of network activity
- Pupil Safeguarding surveys
- Evaluation of children's work
- Pupil discussions at. school council
- Monitoring planning and evidence of work

Key Responsibilities

The Governing Body

- Ratify the Online Safety Policy
- Nominate an Online safety governor who will work with the ICT coordinator as well as other leadership team members and report back to the appropriate Governing Body committee
- Monitor the progress of Online Safety 'Across the Curriculum'.
- Monitor the progress of Online Safety improvement within the Academy

Senior Leadership Team

- The Headteacher and E Safeguarding leader are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Monitor the effectiveness of the Online Safety strategy in raising standards of achievement
- The Headteacher is responsible for ensuring that the online safety team and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Technician

Primary Technology provide our technical support
The school technician ensures:

- That the school's ICT infrastructures are secure and not open to misuse or malicious attack.
- That she/he keeps up to date with online safety technical information and updates the Online Safety Coordinator as relevant.
- That monitoring software, filtering systems, wifi networks and antivirus software are implemented and updated as required

Online Safeguarding Manager

- Takes day to day responsibility for online safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- Attends the relevant Governors meetings where online safeguarding issues are discussed.

Designated Safeguarding Lead for Child Protection

The named person responsible for child protection is trained in online safety issues and is aware of the potential for serious child protection issues that may arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate contact with adults/strangers
- Potential incidents of grooming and/or radicalisation
- Online bullying

ICT Co-ordinator role

- To work with the senior leadership team to develop a robust strategy for dealing with Online Safety across the curriculum
- That the school's IT infrastructure is secure and is not open to misuse or malicious attack
- That monitoring software and anti-virus software is implemented and updated
- That he keeps up to date with online safety technical information and updates the online safety leader or IT Leader as relevant
- To ensure the effective development and implementation of a whole academy Online Safety policy
- To provide INSET opportunities and resources for teachers and support staff as appropriate
- To monitor the implementation of the policy and its effectiveness in raising achievement
- To evaluate the strategy and make modifications as necessary

Teachers and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Online Safety leader for investigation
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Digital communications with students / pupils should be on a professional level and only carried out using official school systems
- Ensure that confidential files are saved in an encrypted file and that the password for this file remains confidential.
- Encourage and reinforce consistent standards of Online Safety use by pupils
- Report any Online Safety matters to the named person immediately in order for it to be dealt with

All Staff and the Online Safety Policy

- All staff will have access to the Academy Online Safety Policy. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff that has a mobile phone within the academy should ensure that they are kept out of sight from pupils and that they have a secure lock on them.

Children

- Are responsible for using the school IT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Report any Online Safety matter to their class teacher, learning leader or phase manager immediately.

Parental/Carer Involvement:

We recognise the strength of staff, pupils and parents/carers all working together. The school will take every opportunity to help carers / parents to understand issues related to online safety. We will assist parents to understand key issues in the following ways:

- Parents/carers will be encouraged to support their son/daughters to be safe online at home
- Parents/carers will be invited into the academy for specific Online Safety events
- At times support outside the classroom for individual pupils may be requested, and we would seek parental/carer support in this

- Parents are asked to review the letter regarding digital and video images and opt out of having images taken and or published on the school web site or blog if they wish to do so
- Regular newsletters and communication offer parents advice on the use of the internet and social media at home

Community Users/Visitors

Community Users/ visitors and volunteers will inform the Principal or Deputy Head of any web sites they wish to access. No person can log on to the internet without a user account or the Internet password. A community user account with minimal privileges will be given after discussion of the sites they wish to access.

Pupil Education

The education of pupils in Online Safety is a crucial part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and to build their awareness of how to keep themselves safe.
Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Online Safety rules will be posted in all networked rooms and key areas.
- Key online safety messages are reinforced as part of a planned programme of assemblies, delivered as part of PHSE and re-enforced during class discussion.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught how to search for information safely and safe search engines are used by Teaching Staff.
- Pupils know that any events of online bullying are taken seriously by the school and they understand the importance of sharing their concerns with a trusted adult
- Pupils are made aware of the process to follow if they see anything online which they find upsetting or which is unsuitable for children.

Staff Training

It is essential that all staff receive regular Online Safeguarding training and that they understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Annual Online Safety staff training
- An annual survey of staff Online Safety training will be completed and any training needs identified.
- The annual questionnaire results from Parents and Pupils will highlight issues relevant to the school and particular year groups. These will be used to direct training.
- Planning and online safety work will be monitored regularly and will be used to direct training.
- All staff will read and ensure they fully understand the Acceptable use policy and Online Safeguarding Policy and Child Protection Policy.

Governor Education

Governors are invited to take part in annual Online Safeguarding training sessions with staff. These are delivered by the Online Safety Coordinator or by a member of the Bradford Curriculum Innovation team. Governors are aware of online safeguarding updates through regular Online Safeguarding Committee meetings or through meetings with the Online Safety Coordinator.

Information Provision

The school Internet is provided by the Bradford Learning Network, a DFE accredited educational Internet service provider. All sites are filtered using a filtering system which generates reports on user activity.

Technical Security

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)
- Access to personal data is securely controlled in line with the school's GDPR policy
- There is effective guidance and training for users
- There are regular reviews and audits of the safety and security of school computer systems
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- All users will have clearly defined access rights to school technical systems as detailed in network and Smoothwall profiles.
- The Computing Co-ordinator is responsible for ensuring that software licence logs are accurate and up to date

Filtering

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school.

All users have a responsibility to report immediately to the Online Safeguarding coordinator any infringements of which they become aware or any sites that are accessed, which they believe should have been filtered.

Monitoring

The school uses a forensic monitoring software solution that records incidents of inappropriate and illegal behaviour which may be carried out by users. This includes searches, other internet activity and also records keystrokes in programmes. Reports are sent to the Principal and Online Safeguarding coordinator. These are logged and appropriate action is taken. These are discussed at online safety committee meetings.

Management of assets

All ICT assets are recorded on an inventory spreadsheet. Assets that are damaged or surplus to requirements have data removed by the Technician before being collected and destroyed by a reputable company. Certificates are received and filed where this has taken place.

Personal Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices such as memory sticks and secure email (e.g Galaxkey)
- Fully understand their responsibilities under GDPR and follow the GDPR policy.

Use of digital and video images (photographic and video)

- Staff should inform and educate pupils about the risk associated with the taking, use, sharing, publication and distribution of images. (Also see Acceptable Use Policy)
- Staff are allowed to take digital/video images to support educational aims (if parental permission has been gained). These images should only be taken on school equipment; personal equipment should not be used for these purposes.
- Parental permission to use photographs on the school website, displays within school and in the press must be given.
- Full names will not be published against pictures on the school website or in displays. In incidences where names are required (some newspapers) parental permission will be

sought.
- Teaching staff are responsible for storing photographs and images safely and securely. Staff will also ensure that images are deleted annually/once the child has left the school.

Passwords

All users (staff and pupils) have the responsibility for the security of their username and password and must not allow other users to access the systems using their log on details (as per Acceptable Use Policies). Any concerns about sharing passwords or log on details must be reported to the Online Safety Coordinator.

- Passwords for new users and replacement passwords for existing users can be allocated by the school technician.
- Members of staff are made aware of the school's password rules through induction, the Acceptable Use Policy and the Online Safeguarding policy.
- All pupils have their own individual log on and password for accessing the school's ICT systems.
- Pupils are made aware of the school's password rules through ICT/Online Safety lessons and through the Pupil Acceptable Use Policy.
- Old usernames and accounts are deleted annually.
- Pupils have individual passwords for logging into the network, and for learning sites such as (but not limited to) PurpleMash, TT Rockstars
- Passwords for logging onto the network are changed annually.
- There is a master list of pupil passwords on a secure drive which is only accessible by the relevant teachers/ IT technician

E-mail

- Only approved e-mail accounts on the academy system.
- Sensitive or identifiable information must only be sent via secure email (such as Glaxykey)
- The forwarding of chain letters is not permitted.
- SLT must be informed immediately of any suspected viral or phishing emails

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However there may be incidents when infringements of the policy could take place. All matters should be reported immediately to the Head/Online Safety Coordinator.

If misuse has taken place it is important that any incidents are dealt with 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.

School may investigate matters that occur outside of school that may affect the safety and wellbeing of children and staff

Online Bullying

Online bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, texting, use of other mobile or tablet apps, email or online software.

- Pupils are taught about online (cyber) bullying through Online Safety, PSHE lessons and awareness sessions provided annual by a police officer.
- Pupils are encouraged to share concerns of online bullying with a trusted adult.
- Pupils and adults who feel as if they are being bullied in any way need to report the matter to SLT.
- Make sure you keep any evidence of online bullying by taking screen captures. Make a note about the time and date of any of these messages and any details about the sender.
- Do not forward messages to other people, this means you are joining in the bullying. Stop it by reporting it to a trusted adult.
- Do not reply to any bullying messages, this could make things worse and shows the bully that they are getting a response from you.

The school may report serious online bullying incidents to the Police. Please see our school Anti Bullying Policy.

Social Media

- As part of our web site pupils are able to comment on posts. All comments are moderated by staff members before they are published.
- All members of staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school.
- The *school's* use of social media for professional purposes will be checked regularly by the online safety committee to ensure compliance with the Social Media, Data Protection, Digital Image and Video Policies.
- The contact details on the Web site will only be the academy address, e-mail and telephone number. Staff or pupils' personal information will not be published.

Mobile Phones

Staff must not use mobile phones or personal devices during lessons or whilst on playground duty. Please refer to the Mobile Policy

School mobile devices

The school has a variety of mobile devices including iPads. All of the statements included in the Acceptable Use Policy also apply to these mobile devices. This includes off-site use of school equipment (e.g. school trips). Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children.

Failure to Comply

Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be investigated by a senior member of staff.

Declaration of Responsibility

This Online Safety Policy was reviewed and formally adopted by Iqra Academy on

…….. Date

…….. Signed Named Governor

…….. Signed Principal

Named Governor:	Rizwan Aziz
Monitoring the Policy:	Principal
Reporting to:	Governors
Next Review Date:	June 2021