Online Safety Policy

Queensmill School

Approved by:	Freddie Adu	**Date:** 18.01.21
Last reviewed on:	18.01.21	
Next review due by:	Jan 22	

Contents

1.Introduction

Queensmill School recognizes that the Internet, and access to it via a range of technologies, is an attractive and increasingly integral feature of children's learning and entertainment. The school recognizes too that in enabling access to this invaluable resource it has a duty to ensure students are:

- safe from inappropriate content in a range of forms and across technologies
- safe from bullying and harassment of any kind
- safe from crime and anti-social behaviour in and out of school
- secure, stable and careful while online
- able to access teaching and learning remotely through a safe and secure online learning platform

It is the duty of the school to ensure that every child in their care is safe, and that the same safeguarding principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks.

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many technological developments, there is also an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective e-safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Queensmill's E-safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our pupils are prepared to deal with the safety challenges that the use of technology brings.

The E-Safety Policy relates to other policies including those for safeguarding, ICT, remote learning, bullying and for child protection.

The designated person for Child Protection is Mr Freddie Adu

The deputy Child protection Officer(s) Ms Joanna Dziopa and Mr Andy Nowak

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

The headteacher and DSL

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with senior management, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

3.2 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

3.3 All staff

All staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.4 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

4. Teaching and learning

Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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 pupils.

ICT will be used across the school to enhance and extend learning, to engage in interesting and vibrant learning activities and to empower learners so that they play a more active role in managing their own learning experiences.

Internet and digital communications play a role in our remote learning offer through Firefly, our online learning platform.

4.2 Internet use will enhance learning

The school's internet access will be designed expressly for pupil use. Access to the internet is enabled through the LGFL filter and where appropriate, the school will request changes to this filter.

In line with Relationships and Sex Education pupils will be taught to what internet use is acceptable and what is not given and given clear information about what to do if they or anyone within school accesses unsuitable material or content which makes them uncomfortable.

Pupils will be educated in the effective use of the internet. This will have particular emphasis on what information they can and cannot share. There will be education too on the skills of knowledge location, retrieval and evaluation.

Pupils will be shown how to publish and present information to a wider audience.

When accessing remote learning (see remote learning policy), pupils will receive learning via Firefly, our online learning platform. Pupils will have access to their class area where resources are clear and easily accessible for pupils and parents. Teachers can upload a range of resources for learning at home including links to websites, pre-recorded lessons, interactive worksheets, visuals and printable materials.

4.3 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught the importance of cross-checking information before accepting its accuracy.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

Pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- What to do if they access inappropriate content (use of the ‘safety’ button and reporting to an adult)
- How to report unpleasant Internet content e.g. using the CEOP Report Abuse icon (www.ceop.police.uk)

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The school will raise parents’ awareness of internet safety in letters or other communications home, and in information via our website and our online learning platform, Firefly. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Acceptable use of the internet in school

All staff are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet. Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1.

8. Managing Information Systems

Information system security

- School ICT systems security will be reviewed regularly.
- Sophos Antivirus and Malwarebytes Antispam software updates will be ongoing.
- Security strategies will be discussed with the Local Authority.

8.2 E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

The forwarding of chain letters is not permitted.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school will consider how e-mail from pupils to external bodies is presented and controlled.

8.3 Published content and the school web site

The contact details given on the website will be the school address, e-mail and telephone number. Staff or pupil personal contact information will not be published.

The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

8.4 Publishing pupil’s images and work

Written permission will be sought from parent/carers before photographs of pupils are published on the school web site.

Pupils’ full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.

Work can only be published with the permission of the pupil and parents/carers. Pupil image file names will

not refer to the pupil by name.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

8.5 Social networking and personal publishing

Social Network sites and newsgroups will be filtered unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for children and young people. Parents will be invited to attend e-safety workshops aimed at raising their awareness of how to manage online content at home.

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- Notify the senior leadership team or the headteacher about what's happening

8.6 Managing filtering

The school will work with appropriate agencies and partners to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the ICT manager or Head Teacher.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

8.7 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.

The senior leadership team have noted that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones are not permitted to be used in school unless agreed with the Head teacher. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

The use by pupils of cameras in mobile phones will be kept under review.

The use of webcams can only be used with the permission of the headteacher or other senior management.

Games machines including the Sony Play station, Microsoft Xbox and others potentially have Internet access. At school, these devices will only be available 'offline'. Staff will supervise pupils who access such devices.

8.8 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

9. Remote Communications

We allow staff to access the school's ICT facilities and materials remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the ICT manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

9.2 Remote Meetings and Training

When it is necessary for parent, staff and professional meetings (such as annual reviews) or trainings to be held remotely, these must be conducted through Microsoft Teams in line with our safeguarding policy. The ICT manager is to manage the setup of accounts for relevant staff to host meetings through this channel.

Queensmill recommends that staff set up an appropriate space for working remotely and ensure:

- Appropriate dress
- Appropriate background
- Senior management are made aware of scheduled meetings/trainings
- Meetings and trainings are scheduled in appropriate rooms, not accessed by students

9.3 Remote Online Learning

Students can access remote learning through Firefly, our online learning platform. Teachers and relevant staff have received relevant training in this programme. Firefly is a secure channel through which a range of resources for learning at home can be uploaded including links to websites, pre-recorded lessons, interactive worksheets, visuals and printable materials.

Staff must ensure that content is appropriate and follows safeguarding and GDPR guidelines by:

- Using school-approved channels (Firefly and Microsoft Teams)
- Notifying senior management of ‘live’ sessions
- Ensuring appropriate dress by staff and students
- Ensuring any lessons are taking place in an appropriate space
- Content of links and videos are checked before being shared/uploaded
- Recordings of lessons are in line with safeguarding and data protection policies

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school’s terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Owen Bridgeman, ICT Manager

11. How the school will respond to issues of misuse

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year. At every review, the policy will be shared with the governing board.

14. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Remote learning policy

Appendix 1: Acceptable use agreement (staff, governors, volunteers and visitors)

Name of staff member/governor/volunteer/visitor:	
When using the school’s ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school’s reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school’s network • Share my password with others or log in to the school’s network using someone else’s details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I’m not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school’s ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school’s ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**