Queen Elizabeth School

Online Safety Policy

Rationale

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. QEII School has made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their online safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of QEII School's protection from legal challenge, relating to the use of ICT.

The Online Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT / behaviour / anti-bullying / child protection.

Mrs Lesley Dyer (Head Teacher and online safety officer), Mr Matt Malone (ICT coordinator) and Mr Stephen Candy (Digital Media) will take a lead at QEII School in coordinating online safety.

Purpose

This policy is designed and intended to reinforce the Acceptable use policies for Staff and Volunteers, Pupils, Parents/Carer's and provide guidelines and working practices for the effective and safe use of the internet, email and other communications technologies in the school, 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 risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order 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.

Scope of the Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils 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 school online 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 head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students/pupils themselves. These responsibilities are reflected in the Acceptable Use Policies for pupils, staff and volunteers and parents/carers.

The use of 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 / 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 Cyberbullying
- Access to unsuitable video
- 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 online safety policy is used in conjunction with other school policies (e.g. behaviour, antibullying, communication and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils 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 online 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 online safety behaviour that take place out of school.

Roles and Responsibilities

National guidance suggests that it is essential for schools to take a leading role in online safety. Becta in its "Safeguarding Children in a Digital World" suggested: "*That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for online safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too.*"

The Byron Review "Safer Children in a Digital World" stressed the role of schools:
"*One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to*

Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator / Officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Head Teacher and Senior Leaders:

- The Headteacher / Online Safety Co-ordinator.is responsible for ensuring the safety (including online safety) of members of the school community,
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Headteacher / 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 safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Online Safety Coordinator:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant Governors meetings
- reports regularly to Senior Leadership Team Network Manager / Technical staff:

The Network Manager and ICT Co-ordinator are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- the school's filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator/Headteacher / ICT Co-ordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching 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 and practices
- 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 Co-ordinator/Head teacher / ICT Co-ordinator for investigation / action / sanction
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other school activities

Pupils

As far as is reasonable:

- understand and follow the school online safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- in lessons where internet use is pre-planned pupils 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.

Designated person for child protection

Should be trained in online 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

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (nb. For some pupils it would be expected that parents / carers would sign on behalf of the pupils)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy 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 every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

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. At QEII School we therefore believe we have a duty to provide all of our pupils with high-quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.
- Internet use will enhance and extend learning
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate Internet content
- QEII School must ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

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, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments will not be permitted in pupil accounts.
- The forwarding of chain letters is not permitted.

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, QEII School adopts best practice that pupils 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.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded

from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils are carefully selected and comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate 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.

- When personal data is stored on any portable computer system, USB stick or any other removable media:
- The data must be encrypted and password protected
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Unsuitable / inappropriate activities

QEII School believes that the activities listed below would be inappropriate in a school context and those users, should not engage in these activities in school or outside school when using school equipment or systems. 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:

- child sexual abuse images
- promotion or conduct of illegal acts, e.g. 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 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 other safeguards employed by Local Authority 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 (e.g. 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 gambling
- On-line shopping / commerce
- File sharing
- Use of social networking sites
- Use of video broadcasting e.g. YouTube (for personal use)

For further information please refer to Full and Summary Guidance for the Safer Use of the Internet by Staff Working with Young People.

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 are the responses that will be made to any apparent or actual incidents of misuse:
If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, 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. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends 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.

Published content and the school web site

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. The Headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked 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 should not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.

See Social Media Policy for more detail.

Managing filtering

The school will work in partnership with the Local Authority and be guided by the SWGFL to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator or the Network Manager. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing

Video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Pupils should ask permission from the supervising teacher before making or answering a videoconference call. Video conferencing will be appropriately supervised for the Pupil's age.

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 management team should note 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 will not be used during lessons or formal school time, unless as part of a lesson, where directed by a member of staff. The sending of abusive or inappropriate text messages is forbidden.

There will be heavy sanctions imposed on those students who misuse camera phones.

The use by students of cameras in mobile phones will be kept under review. Games machines including the Sony PlayStation, Microsoft Xbox/ PSP and others have Internet access which may not include filtering. Care is required if there is any use in school or other officially sanctioned location (classrooms – only with supervised use or the Sensory studio – again only supervised used)

Should staff need to contact parents on their mobile phone, the Headteacher should be informed and a valid reason given. The Headteacher will maintain a log of which parents have access to staff mobile phones.

More information is available on the school server.

Protecting personal data

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

Policy Decisions

Authorising Internet access

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
Where appropriate, secondary pupils must apply for Internet access individually by agreeing to comply with the Pupil Acceptable Use Policy.

Parents / carers will be asked to sign and return the Parent / Carer Acceptable Use Policy.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school should audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to online safety.

Communicating Online Safety

Introducing the online safety policy to pupils

Online Safety rules will be posted in all rooms where computers are used. Pupils will be informed that network and Internet use will be monitored. A programme of training in Online Safety will be developed, possibly based on the materials from CEOP and similar agencies.

Staff and the Online Safety policy

All staff will be given the School Online Safety Policy and its importance explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship. Staff are asked not to have pupils as 'friends' on social networking sites and to be cautious when 'befriending' parents.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school Web site. The school will maintain a list of online safety resources for parents/carers. Parents and carers will be expected to read and sign up to an acceptable use policy for their young person in school.

Resources

The school's ICT and computer network systems. Internet access as provided by the EXA.

Equal Opportunities

The school supports the right of all staff and pupils to equal access and chances regardless of age, ethnicity, gender, social circumstances, ability / disability or sexuality.

Health & Safety

Health & Safety issues are described fully in the School Health & Safety Policy. It is the responsibility of each adult to report health & safety issues without delay.

Professional Development

All staff are provided with training opportunities to deliver the curriculum including special requirements to meet the needs of pupils where appropriate. Training needs will be linked to Performance Management, staff interviews and the School Improvement Plan.