Queen Elizabeth School

E-Safety Policy

Rationale

The requirement to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been show to raise educational standards and promote pupil / 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
- Un-authorised 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
- Cyber-bullying
- Access to unsuitable video / internet games
- 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 used in conjunction with other policies including those for ICT / behaviour / anti-bullying / child protection.

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 which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

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.

1. Development and Monitoring

Role	Named Person
Computing Subject Co-ordinator	Rachel Branigan
Designated Safeguarding Lead	Victoria Harrington
Digital Media	Stephen Candy

This e-safety policy has been developed by the Computing Subject Co-ordinator and the Designated Safeguarding Lead in conjunction with the school Senior Management Team. As part of this policy, records will be maintained of e-safety related incidents involving staff and pupils and any incidents will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

The school will monitor the impact of the policy using:

- Feedback from staff, pupils, parents / carers, governors
- Logs of reported incidents
- Internet activity monitoring logs

2. 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 policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school and 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.

3. Roles and Responsibilities

Governors:

Governors are responsible for the approval of the e-safety policy and for reviewing its effectiveness.

Headteacher and Senior Management:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, through the day to day responsibility for e-safety will be delegated to the Computing subject co-ordinator and Designated Safeguarding Lead
- The Headteacher is responsible for the implementation and effectiveness of this policy. She is also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement
- The Headteacher / Senior Management are responsible for ensuring that the Computing Subject Co-ordinator / Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles
- The Headteacher / Senior Management will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on the important monitoring roles.
- The Headteacher and another member of the Senior Management Team should be aware of the prcdeures to be followed in the event of a serious e-safety allegation being made against a member of staff. (refer to Managing Allegations against a member of staff guidance)

Computing Subject Co-ordinator and Designated Safeguarding Lead:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Reports to the School Management Team serious breaches of the e-safety policies
- Provides training and advice for staff
- Liaises with the Local Authority
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Are trained in and shares with staff an awareness and understanding of e-safety issues and the potential for serious child protection issues that can arise from:
  - Sharing of personal data
  - Access to illegal / inappropriate materials
  - Inappropriate on-line contact with adults / strangers
  - Potential or actual incidents or grooming
  - Cyber-bullying
  - Sexting
  - Revenge pornography

- Radicalisation (extreme views)
- CSE

The Network Manager and Computing Subject 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

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood the e-safety policy, school Acceptable Use policy
- They report and suspected misuse or problems to the Computing Subject Co-ordinator / Designated Safeguarding Lead for investigation / action / sanction
- Digital communications with pupils and parents / carers (email/voice) should be on a professional level
- Students / pupils understand and follow, as appropriate for age and ability, the school e-safety and acceptable use policy
- Students / pupils understand and follow e-safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our behaviour and anti-bullying policies
- In lessons where internet use is planned students / 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.

Pupils:

- Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to agree to 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)

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability
- 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 e-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 / local e-safety campaigns / literature.

Parents and carers will be responsible for:

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

Parents/carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

4. Education and Training

Education – Pupils

E-safety education will be provided in the following ways, as appropriate to pupils' age and ability:

- A planned e-safety programme should be provided as part of Computing / PSHE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devise both within and outside school
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils are taught the importance of keeping information such as their password safe and secure

- Rules for the use of ICT systems / internet will be made available for pupils to read
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Students / pupils are taught how to keep safe through effective / good e-safety practice as part of an integral elements of the school Computing curriculum and within their ICT learning
- Where students / pupils are allowed to freely search the intranet, 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, students 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.

Education – Parents and Carers

Many parents and carers have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-lines experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report)

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, web site
- Parents evenings
- Reference to external e-safety websites
- High profile events such as Internet safety day
- Family learning opportunities

Education and Training -Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school e-safety policy and Acceptable Use Policies
- The Computing Subject Co-ordinator (or other nominated person) will proved advice / guidance / training to individuals as required.

5. Technical – Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed through the managed service provider, in ways that ensure that the school meets the e-safety technical requirement for West Sussex Local Authority
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- Staff will be made responsible for the security of their username and password, must not allow other users to access the system using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports the managed filtering service provided by service provider. Any incidents or activities regarding filtering will be handled in accordance with WSSfS
- Remote management tools are used by the managed service provider to control workstations and view users activity
- Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- Guest can access the school network using the guest login, guests will not give access to personal information about pupils or staff
- The school infrastructure and individual workstations are protected by up to date anti-virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy

6. 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 students / 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 or social media.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

7. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the school Personal Data Guidance.

8. Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the Designated Safeguarding Lead – the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include an unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer.

9. 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 U
- 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.

10. 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 by pupils, staff or any other user 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 incident should be following in accordance with the safeguarding policy and is necessary, the police should also be informed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather that 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.

11. Monitoring and review

This policy will be reviewed annually, or earlier if necessary in line with national and/or local updates.