Name of Policy: E-SAFETY

Date approved: August 2022

Date for Review: August 2024

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 students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of contextto 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 towhich all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raiseeducational standards and promote student achievement. However, the use of these new technologiescan 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
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development andlearning 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 school policies (e.g. Behaviour for Learning, Anti-bullying 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 students' resilience to the risks to whichthey 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 havedone everything that could reasonably be expected of them to manage and reduce these risks. The e- 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.

E-Safety Coordinator Roles and Responsibilities:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing andreviewing the school e-safety policy.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides opportunities for training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with the e-safety governor and E-Safety Committee to discuss current issues, review incident logs and filtering/change control logs.
- Reports to the School Steering Committee.
- Decides how specific incidents will be dealt with.
- Applies investigation/action/sanctions.
- Is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from sharing of personal data, accessing illegal/inappropriate materials, inappropriate on-line contact with adults/strangers, potential or actual incidents of grooming, cyber-bullying.

Network Manager/Technical Staff Roles and Responsibilities:

- Ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Ensure that the school meets the e-safety technical requirements outlined in the Network Security Policy and Acceptable Usage Policy and any relevant Local Authority e-safety policy and guidance.
- Ensure that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Ensure that Network is informed of issues relating to the filtering applied by the Grid
- Ensure that the school's filtering policy is applied and that it is updated on a regular basis.
- Ensure that he keeps up to date with e-safety technical information in order to effectively carry out his e-safety role, and to inform and update his team as required.
- Ensure that the use of the network/Virtual Learning Environment/remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator or another member of the Steering Committee for investigation/action/sanction.
- Ensure that monitoring software/systems are implemented and updated as agreed in school policies.

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 thatpolicies and procedures approved within this policy are implemented.
- The relevant people will be effective in carrying out their e-safety responsibilities.
- The school meets the e-safety technical requirements outlined in the Network Security Policy and Acceptable Usage Policy and any relevant Local Authority e-safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded and reviewed accordingly, by the E-Safety Committee.
- All users will be provided with a username and password by the Network Manager who willkeep an up to date record of users and their usernames.

- The administrator passwords for the school ICT system, used by the Network Manager (andtechnicians) are available to the Principal and are kept in a secure place. Sole administrative access is not in occurrence.
- Users are made responsible for the security of their username and password.
- The school maintains and supports the managed filtering service provided by Network.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by thePresident of the Board (or other nominated senior leader).
- Any filtering issues should be reported immediately.
- Requests from staff for sites to be removed from the filtered list will be considered by the NetworkManager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wirelesssystems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/ community users) and their family members are allowed on laptops and other portable devices owned by the school that may be used outside of the school.
- An agreed policy is in place that forbids staff from installing programmes on school workstationsor portable devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs)by users on school workstations/portable devices
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted orotherwise secured.

Curriculum

E-safety is a focus in all areas of the curriculum and staff should reinforce e-safety messages in theuse of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should bevigilant 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 researchtopics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (or technicians) 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.
- Students are taught in all lessons to be critically aware of the materials/content they access on-lineand be guided to validate the accuracy of information.
- Students 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, allowingstaff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students 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 andexisting employees. The school will inform and educate users about these risks and will implementpolicies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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 students are appropriately dressed andare not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selectedcarefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in associationwith photographs.
- Written consent from Parents/Guardians has be obtained on admissions for publishingphotographs of students on school publications.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the DataProtection 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.

As a school we will:

- 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 thatthey 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 otherremovable media:

- The data must be encrypted and password protected.
- Where possible the device must 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 once it has been transferred or its use is complete.

Please refer to the schools Data Protection Policy for further details.

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users are all aware that email communications are monitored and filtered.
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature to a member of the E-Safety Committee, and must notrespond to any such email.
- Any digital communication between staff and students or parents/carers (email, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students are taught about email safety issues, such as the risks attached to the use of personal details.They are also taught strategies to deal with inappropriate emails and are reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Unsuitable/Inappropriate Activities

Some internet activity (e.g. accessing child abuse images or distributing racist material) is illegal and would therefore result in a ban from all school ICT systems, until proceedings for a criminal investigation had taken place. Other activities (e.g., cyber bulling or accessing pornography) may not be illegal, but are obviously inappropriate in the school context. These activities will lead to a ban from all school ICT systems until the relevant member/s of the E-Safety Working Party have completed an investigation, and the issue is resolved.