King Edward VI School

Online Safety Policy

November 2016

To be reviewed annually

Adopted at Governing Body meeting on……23 November 2016

Signed……Brian Field……..

Date ……23/11/16……

1. Principles

- 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 context to promote effective learning. Children and young people have an entitlement to safe internet access at all times.
- The use of these exciting and innovative tools in school and at home has been shown to help raise standards and promote 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
    - 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
    - Online bullying
    - Promoting illegal acts
    - 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 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 (eg Acceptable Use of ICT, Behaviour, and Safeguarding 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 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 done everything that could reasonably be expected to manage and reduce these risks.

2. Scope

- This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
- The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 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 behaviour that take place out of school.

3. Roles and Responsibilities

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. A member of the Governing Body will take on the role of Online Safety Governor.
- The role of the Online Safety Governor includes regular meetings with the Online Safety Lead with the school's Designated Senior Lead (Safeguarding) to discuss current issues and monitor online incidents.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their role and to train other colleagues, as appropriate
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Headteacher and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious allegation being made against a member of staff.

Online Safety Lead:

- Takes day to day (managed by the school's Designated Senior Leads) responsibility for online issues and has a leading role in establishing and reviewing the school policy
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority and Police
- Liaises with school IT technical staff.
- Receives reports of online incidents and ensures a log is kept of incidents to inform future developments.
- Meets regularly with the Online Safety Governor and Designated Senior Leads to discuss current issues and review incidents.
- Reports to the school's Senior Designated Leads (for Safeguarding and Child Protection).

IT Manager/IT Support Staff 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 online safety technical requirements
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with online safety technical information in order to effectively carry out their role and to inform and update others as relevant
- Regular monitoring of internet / change control logs and reporting to Online Safety Lead / Senior Leaders as appropriate
- That the use of the school's network, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the IT Manager who would then refer on as appropriate to either the Online Safety Lead or Senior Leaders.

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 policy and practices
- They have read, understood and signed the school Acceptable Use of ICT Policy/Agreement form
- They report any suspected misuse or problem to the IT Manager/Online Safety Lead for investigation and action;
- Digital communications with students (email/internet based) 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
- Students understand and follow the school online safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor IT activity in lessons, extra-curricular and extended school activities;
- They are aware of online safety issues related to the use of mobile phones, watches, 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 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
- In class use of mobile phones/devices is controlled via a visual approval system by the classroom teacher.

Senior Designated Lead for Safeguarding:

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
- Online bullying.

Students are responsible for using the school IT systems in accordance with the IT Agreement, which they will be expected to sign before being given access to school systems

- 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 policy on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policy on the taking/use of images and on online bullying
- Should understand the importance of adopting good online 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 IT than their children. The school will therefore take every opportunity to help parents/carers understand these issues through consultation evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student IT Agreement
- Accessing the school website/online student records in accordance with the relevant school Acceptable Use Policy.

4. Policy Statements

Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's safeguarding provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety education will be provided in the following ways:

- Key online safety messages will be reinforced in assemblies and tutorial activities
- Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information

- Students should be encouraged to adopt safe and responsible use of IT, the internet and mobile, watches and handheld devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of IT, the internet and mobile, watches and handheld devices.

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

- Information evenings
- Individual conversations
- In newsletters and other suitable material.

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
- School IT systems will be managed in ways that ensure that the school meets the online safety technical requirements
- There will be regular reviews and audits of the safety and security of school IT systems
- Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to school IT systems this is reviewed according to changing requirements.
- All users will be provided with a username and password.
- The ‘master/administrator’ passwords for the school IT system, used by the Network Manager will also be available to the Headteacher and kept in a secure place
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains internet filtering provided by McAfee
- In the event of the IT 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 the Headteacher
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager / IT support staff
- School IT support staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy.

- Remote management tools are used by the IT Manager / IT Support Staff to control workstations and view user's activity, this includes keyword monitoring functionality.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- The school infrastructure and individual workstations are protected by up to date antivirus software.

6. 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 freely to search the internet, staff should be vigilant in monitoring the content of the websites that students visit
- It is accepted that from time-to-time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager or IT Support Staff temporarily remove those sites from the filtered list for the period of study. Any request to do so should be in writing with clear reasons for the need
- Students should be taught in all lessons to be critically aware of the materials/content they access online and 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.

7. Use of digital and video images

- 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 eg on social networking sites
- Staff are allowed to take digital/video images to support educational aims, but must follow school policy 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 and are 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 or their parent / carer's consent

- Students' names / photographs will not be used online without consent from their parent / carer's consent. Permission is obtained on admission to the school.

8. Data Protection

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

9. Responding to incidents of misuse

- It is hoped that all members of the school will be responsible users of IT, 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
- Student misuse will be dealt with through the school's behaviour management procedures, unless there are legal or child protection concerns, in which case the incident will be reported to the relevant outside agencies, such as the police or social services
- Staff misuse will be dealt with through the school and Local Authority's disciplinary procedures.