eSafety Policy

Introduction

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. A school eSafety 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 Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational 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
- 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 and learning of children.

Many of these risks reflect situations in the off-line world and it is essential that this eSafety policy is used in conjunction with other school policies (e.g. behaviour, 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 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.

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 these risks. The eSafety 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.

Monitoring/Review of this Policy

This eSafety policy will be monitored and reviewed by a working group made up of:

- Headteacher
- Governors

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, 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 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 eSafety 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 eSafety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for eSafety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Pastoral Committee receiving information about eSafety incidents.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including eSafety) of members of the school community,
- The Headteacher is responsible for ensuring that staff receive suitable CPD to enable them to carry out their eSafety roles and to train other colleagues, as relevant.
- The Headteacher should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff. (see the flow chart on dealing with eSafety incidents – included in a later section – "Responding to incidents of misuse")
- The Head teacher delegates to Lexicon the technical aspects of the following but assumes the reponsibility for:
    - ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
    - ensuring that the school meets the eSafety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority eSafety Policy and guidance
    - ensuring that users may only access the school's networks through a properly enforce password protection policy, in which passwords are regularly changed
    - ensuring that the SWGfL is informed of issues relating to the filtering applied by the Grid
    - the school's filtering policy, 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 eSafety technical information in order to inform the Head teacher so that she can effectively carry out their eSafety 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 Headteacher for investigation/action/sanction
    - that monitoring software/systems are implemented and updated as agreed in school policies
    - establishing and reviewing the school's eSafety policies and documents
    - liaising with the Local Authority

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of eSafety matters and of the current school eSafety 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 ICT Technician/eSafety Officer/ Headteacher for investigation/action/sanction
- any digital communications with pupils or parents/carers (email/Virtual Learning Environment (VLE)/ chat/ online gaming) should be on a professional level. 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
- eSafety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school eSafety and acceptable use policy
- 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 eSafety 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 persons for child protection/Child Protection Officer

should be trained in eSafety 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

Pastoral and Curriculum Committee

Members of the Pastoral Committee will assist the eSafety Officer with:

- the production/review/monitoring of the school eSafety policy/documents

- the production/review/monitoring of the school filtering policy.

Pupils/pupils:

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a developing understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- will be encouraged to report abuse, misuse or access to inappropriate materials
- will be informed about school policies on the use of mobile phones, digital cameras and hand held devices. They will be informed about school policies on the taking/use of images and on cyber-bullying.
- will develop an understanding of the importance of adopting good eSafety practice when using digital technologies out of school and realise that the school's eSafety

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 and information about national/local eSafety campaigns/literature.

Policy Statements

Education – pupils

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

eSafety education will be provided in the following ways:

- An eSafety programme should be provided as part of ICT/PHSE/other lessons – this will cover both the use of ICT and new technologies in school and outside school

- 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 helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils 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 ICT, the internet and mobile devices

Education – parents/carers

Many parents and carers have only a limited understanding of eSafety 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-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful an 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, newsletters, web site
- Parents' evenings

Education & Training – Staff

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

- All new staff should receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Policies
- The Head teacher will keep up to date by reviewing guidance documents released by SWGfL/LA and others.
- This eSafety policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.

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 eSafety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the eSafety technical requirements outlined in the SWGfL 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 will have clearly defined access rights to school ICT systems
- The "administrator" passwords for the school ICT system is kept in a secure place
- Users will be made responsible for the security of their username and password. They 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 and supports the managed filtering service provided by SWGfL.
- Any filtering issues should be reported immediately to the Head teacher
- Appropriate security measures are in place 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.
- An agreed policy is in place (Laptop / ipad Agreement) regarding the extent of personal use - that users (staff/pupils/community users) and their family members are not allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place (Laptop Agreement) that forbids staff from installing programmes on school workstations/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 antivirus software.

Curriculum

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

- in lessons where internet use is pre-planned, it is 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.

- 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 will be selected carefully and will 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.
- Student's work can only be published with the permission of the student 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.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
- the data must be password protected
- the device must offer approved virus 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

Signed Chair of Governors

Date

This policy was agreed by Governors on 20th October 2016

It will be reviewed on 20/10/17