Online Safety Policy

Adopted:	12 May 2016
Review Date:	Summer 2017
Responsible for Review:	Network Manager
Committee for Review:	Steering
Frequency of Review:	1 Year
Statutory:	No

Contents

Introduction

The development and expansion of the use of Information and Communications Technologies (ICT), and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have 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 the school's protection relating to the use of ICT.

Background / Rationale

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 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 Online Safety Policy should help to ensure safe and appropriate use. The development and implementation of such a strategy involves 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 students 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 or radicalisation 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 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. Learning Expectations, Anti-bullying 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.

Development / Monitoring / Review of this Policy

This Online Safety Policy has been developed by a working group; the Online Safety Committee members are:

- Online Safety Coordinator (Rick Hekkenberg)
- Headteacher (Angelo Goduti)
- Online Safety Governor (Matthew Zipfel)
- Designated Safeguarding Lead

The implementation of this Online Safety Policy will be monitored by the Online Safety Committee

- Monitoring will take place at regular intervals e.g. at least annually or as appropriate.
- The Governing Body and/or Governors Sub Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals e.g. annually.

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School / Student Council
- INSET Day
- Governors' meetings
- Teaching & Learning Committee meeting
- Parents' evenings
- School website / newsletters

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place.

Should serious Online Safety incidents take place, the Safeguarding Officer (Associate Headteacher) should be informed.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of students (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
- Parents / carers
- Staff

Scope of the Policy

- 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 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 Learning Expectations and Anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that takes place out of school.

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. 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
- regular monitoring of Online Safety incident logs
- reporting to relevant Governors meetings

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training 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 Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff. (See flow chart on dealing with Online Safety incidents).

Online Safety Coordinator:

- leads the Online Safety committee
- 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 Online Safety Governor to discuss current issues, review incident logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

ICT Technical staff:
The ICT technical staff are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Senior Leaders are informed of issues relating to the filtering applied by IT Services
- 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 he/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 for investigation/action / sanction
- that monitoring software/systems are implemented and updated

Teaching and Support Staff:
The 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 for investigation/action/sanction
- digital communications with students (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
- 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 ICT activity in lessons, extra-curricular and extended school activities, making regular checks during lesson time of student use

- 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 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

Designated Person for Safeguarding:
The Senior Designated Officer for Safeguarding is trained in Online Safety issues and is aware of the potential for serious safeguarding issues which may 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

Online Safety Committee:
Members of the Online Safety committee (or other relevant group) will assist the Online Safety Coordinator (or other relevant person, as above) with:

- the production / review / monitoring of the school Online Safety policy / documents.
- the production / review / monitoring of the school filtering policy

Students:

- 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 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 school blog. Parents and carers will be responsible for:

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

Policy Statements

Education – Students

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 Online Safety 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:

- A planned Online Safety programme should be provided as part of ICT, PHSEE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies, tutorial and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student acceptable use policy/ agreement (AUP) and encouraged to adopt safe and responsible use of ICT, the internet and mobile 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
- Rules for use of ICT systems/internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents/carers

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

- Letters, newsletters, web site, VLE
- Parents evenings

Education - Extended Schools
The school will offer family learning courses in ICT, media literacy and Online Safety so that parents and children can together gain a better understanding of these issues. Messages to the public around Online Safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff
It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to staff. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety and Acceptable Use Policies
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by LA and others
- This Online Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The Online Safety Coordinator (or other nominated person) will provide advice/guidance/ training as required to individuals as required

Training – Governors
Governors should take part in Online Safety training awareness sessions, with particular importance for those who are Online Safety/Health and Safety/Safeguarding links. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority
- Participation in school training/information sessions for staff or parents

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 Online Safety responsibilities:

- School ICT systems will be managed in ways that ensure 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
- 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. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Committee
- All users will be provided with a username and password by IT Services who will keep an up to date record of users and their usernames. Users will be required to change their password every 30 days. **Passwords must contain a combination of uppercase and lowercase letters and either number(s) or special character(s) (i.e. Norwich1 or Norwich@). First or last names cannot be used. The last five passwords are remembered."**
- The "administrator" passwords for the school ICT system used by IT Services must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- 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 and supports the filtering solution provided by Censornet
- 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 the Headteacher (or other nominated senior leader)
- Any filtering issues should be reported immediately to IT Services
- Requests from staff for sites to be removed from the filtered list will be considered by IT Services. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Remote management tools are used by staff to control workstations and view users' activity
- An appropriate system is in place for users to report any actual/potential Online Safety incident to IT Services
- 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 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 and community users) and their family members are allowed on laptops and other portable devices that may be used out of school
- An agreed policy is in place 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 virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

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, 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 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
- Students 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
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet by referencing their sources in an acceptable format

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff 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 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 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 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 permission
- Photographs published on the website, or elsewhere that include students will be selected carefully 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 association with photographs
- Written permission from parents/carers will be obtained before photographs of students are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year)
- Student's work can only be published with the permission of the student and parents/ 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

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√						√	
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√							√
Taking photos on mobile phones or other camera devices				√				√

Use of hand held devices eg PDAs, PSPs	√							√
Use of personal email addresses in school, or on school network	√							√
Use of school email for personal emails		√						√
Use of chat rooms / facilities				√				√
Use of instant messaging	√							√
Use of social networking sites				√ *				√**
Use of blogs	√					√		

* Staff need to sign Social Media Account Request Form
** This can be temporarily enabled by teaching staff. For example for media or art students.

Unsuitable / Inappropriate Activities
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and
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 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 (eg 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 thei use of the internet				√	
On-line gaming (educational)	√				
On-line gaming (non-educational)				√	
On-line gambling				√	
On-line shopping / commerce				√	
File sharing				√	
Use of social networking sites			√*		
Use of video broadcasting e.g. Youtube			√		

* This can be temporarily enabled by teaching staff. For example for media or art students.