E-SAFETY POLICY

Date written: January 2018
Review date: January 2019

E-Safety Policy

Introduction & Context

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 e-safety (electronic safety) 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 head teacher 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 pupil 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
  - Access to terrorism and extremism
- 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 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 and relationships, learning and teaching and safeguarding policies).

As with all other risks, it is impossible to eliminate them 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 them.

As a school it is necessary we provide safeguards to help ensure that we have done everything that could reasonably be expected of us, to manage and reduce these risks. The e-safety policy that follows, explains how we intend to do this, whilst also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe when using the Internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, governors, 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 Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils not only when they are onsite but also when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is relevant to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.
The school will deal with such incidents in accordance with the behaviour and relationships policy and inform parents/carers of incidents of inappropriate e-safety behaviour that take place both in and out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the ICT Co-ordinator;
- regular monitoring of e-safety incident logs;
- reporting to relevant Governors meeting.

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT Co-ordinator;
- The SLT are responsible for ensuring that the ICT Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
- The SLT 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 support to those colleagues who take on monitoring roles. The school has adopted Central Policies software to monitor Users work in school;
- The SLT will receive regular monitoring reports from the ICT Co-ordinator;

- The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff - see relevant LA guidelines.

ICT Co-ordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and 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;
- provides training and advice for staff;
- 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 E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs;
- attends relevant meetings of Governors;
- reports regularly to SLT.

Network Manager and Technical staff:

The ICT Technician and ICT 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 e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance;
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed;
- 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 (see LA guidelines);
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the ICT Co-ordinator for investigation, action or sanction;
- that monitoring software / systems are implemented and updated.

Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read and understood the school E-Safety Policy.
- they report any suspected misuse or problem to the ICT Co-ordinator for investigation, action or sanction;
- digital communications with pupils should be on a professional level and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other school activities;
- pupils understand and follow the school e-safety and age-appropriate 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 e-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 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 Safeguarding Officer:

- should be trained in e-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;
  cyber-bullying.

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they are asked to accept each time they log onto the school network;
- have a good age-appropriate 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 e-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, school website and information about both national and local e-safety campaigns / literature.

Governor / Volunteer / Community Users:

- These users who access school ICT systems / website as part of the Extended School provision will be expected to follow the relevant Acceptable User Policy before being provided with access to school systems.

Policy Statements

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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of the curriculum 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 a planned programme of assemblies and classroom activities;
- 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 pupil 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;
- Rules for use of ICT systems / Internet will be posted in all relevant rooms;
- Staff should act as good role models in their use of ICT, the Internet and mobile devices.

Parents / Carers:
Many parents and carers have only 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-line 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. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters,
- website,
- reference to the 'Thinkuknow' & 'CEOP' websites
- Parents evenings

Education & 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 the school e-safety policy and Acceptable Use Policies;

- The ICT Co-ordinator will receive regular updates through attendance at LA training sessions and by reviewing guidance documents released by BECTA* / LA and others;
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days;
- The ICT Co-ordinator will provide advice / guidance / training as required to individuals.

Governors:
Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation;
- 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 e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the 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. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the ICT Coordinator;
- All users will be provided with a username and password by (IBS technician) who will keep an up to date record of users and their usernames. Pupil's passwords will be changed regularly with Year 6 pupils having individual passwords;
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher and ICT Coordinator 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 and supports the managed filtering service provided by the LA;
- The school has provided enhanced user-level filtering through the use of the Central Policies filtering software;
- 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 Head teacher or ICT Coordinator;
- 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 e-safety incident to the ICT Coordinator; This also protects children from any access to terrorism and extremism online.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices from accidental or malicious attempts which might threaten the security of the school systems and data;
- An agreed policy is in place regarding the downloading of executable files by users for teaching purposes;
- An agreed policy is in place regarding the extent of personal use that staff allowed on laptops and other portable devices that may be used out of school. Laptops provided by the school must be used primarily for work relating to school;
- The school infrastructure and individual workstations are protected by up to date virus software;
- Personal data can not be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured, (Data Protection Act).

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety 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 pupils 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 or ICT Coordinator 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;
- 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;
- 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 the website particularly in association with photographs;
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website;

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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. 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 password protected;
  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 once it has been transferred or its use is complete.

Communications

This is an area of rapidly developing technologies and uses which 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				Pupils			
Communication Technologies	Allowed	Allowed at certain	Allowed for selected	Not allowed	Allowed	Allowed at certain	Allowed with staff	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			√					√
Taking photos on camera devices	√				√			
Use of personal email addresses in school, or on school network		√						√
Use of school email for personal emails	√				√*			
Use of chat rooms / facilities / instant messaging / social networking sites				√				√
Use of blogs for curriculum uses	√				√*			

* Staff may use mobile phones in school but must adhere to the AUP guidelines.
* Pupils may bring mobile phones into school but must adhere to the AUP guidelines.
* Pupils may use school email in accordance with the school guidelines.
* Pupils can use blogs for curriculum purposes once they have received appropriate teaching.

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 pupils should use it in accordance with school guidelines;
- Users need to be aware that email communications are monitored;
- Users must immediately report 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 pupils or parents / carers must be professional in tone and content. Public chat / social networking programmes must not be used for these communications;
- Whole class or group email addresses will be used at KS1, and lower KS2, while pupils in upper KS2 will be provided with individual school email addresses for relevant educational use;
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be 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 obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and those 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: *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:*	Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
child sexual abuse images					√
promotion or conduct of illegal acts; eg 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				√	

User Actions: *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:*	Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
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 WCC				√	
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 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 eg Youtube			√		

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 through deliberate misuse.

If any apparent or actual misuse appears to involve illegal activity including:

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;

- other criminal conduct, activity or materials;

then advice will be sought from the LA and police in regards to dealing with the incident. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. School will follow LA guidelines.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. Any incidents will be dealt with quickly, and that the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with using behaviour / disciplinary procedures as follows:

Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher	Refer to KS Leader	Refer to SLT	Refer to Police / Social Services	Refer to technical support staff for	Inform parents /	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√	√	√	√	√		√
Unauthorised use of non-educational sites	√								
Unauthorised use of mobile phone / digital camera / other handheld device	√	√	√						
Unauthorised use of social networking / instant messaging / personal email	√				√				
Unauthorised downloading or uploading of files	√								
Allowing others to access school network by sharing username and passwords	√								
Attempting to access or accessing the school network, using another pupil's account	√								
Attempting to access or accessing the school network, using the account of a member of staff	√	√	√						
Corrupting or deliberating damaging the data of other users	√	√	√			√			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√			√	√		
Continued infringements of the above, following previous warnings or sanctions	√	√	√			√	√		√

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√	√			√			
Using proxy sites or to subvert the school's filtering system	√	√	√		√	√	√	√	√
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√	√		√	√			
Deliberately accessing or trying to access offensive or pornographic material	√	√	√	√	√	√	√	√	√
Receipt or transmission of material that infringes the copyright of another person or the Data Protection Act	√	√	√		√	√			

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to SLT	Refer to Local Authority / HR or Social Services	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√	√	√	√	√	√
Excessive or inappropriate personal use of the Internet / social networking sites / instant messaging / personal email	√	√						
Unauthorised downloading or uploading of files	√	√			√			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	√							
Careless use of personal data eg holding or transferring data in an insecure manner	√	√						
Deliberate actions to breach data protection or network security rules	√	√	√		√			
Corrupting or destroying the data of other users	√	√						
Causing deliberate damage to hardware or software	√	√	√		√			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√					
Using social networking / instant messaging / text messaging to carrying out digital communications with pupils	√	√	√					
Actions which could compromise the staff member's professional standing	√							
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√						
Using proxy sites or other means to subvert the school's filtering system	√	√	√		√			
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√			√			

Deliberately accessing or trying to access offensive or pornographic material	√	√	√					√
Breaching copyright or licensing regulations	√							
Continued infringements of the above, following previous warnings or sanctions	√	√	√			√		√

Useful Acronyms:

ICT – Information Communication Technology

AUP – Acceptable User Policy

BECTA – British Educational Communications & Technology Agency