Belton C of E Primary School

Achieving the best together

E Safety Policy

Date: January 2020

Review date: January 2021

E safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and adults about the benefits and risks of using new technologies and provides safeguards and awareness for users to enable them to control their online experiences. The school's E safety policy works alongside other policies such as the Positive Behaviour policy, Safeguarding and Child Protection, Data Protectionand the staff code of conduct.

Purpose and scope of the e-safety policy

- To educate pupils about e- safety issues and appropriate behaviours so that they remain safe and legal online.
- To help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.
- To keep any personal data and information secure.
- To minimise the risks of handling sensitive information.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband provided by Schools' broadband and Lightspeed filtering

Why is Internet Use Important?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;

- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;

What does electronic communication include?

- Internet collaboration tools: websites, social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones and Tablets / iPads;
- Internet communications: email and instant messaging;
- Webcams and video-conferencing;
- Wireless games consoles.
- chat rooms, social media, blogs, podcasts, downloads, virtual learning platform

What are the risks of internet technologies?

While Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school, it is also important to consider the risks associated with the way these technologies can be used. These risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Incidents will vary from the unconsidered action to considered illegal activity.

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

Pupils with SEN have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. At Belton C of E Primary School, it is our duty of care alongside that of parents and other members of the community to protect all our pupils from these dangers and we are committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children. The purpose of this e-safety policy is to outline what measures the school takes to ensure that pupils can work in an e-safe

environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion. We will use education, technology, accountability, responsibility and legislation as the key ways to achieve this. The school will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies.

Lightspeed Systems filtering ensures that inappropriate websites are blocked and the headteacher receives a weekly 'suspicious reports' report which would alert the school of any inappropriate attempts to access inappropriate websites or material. All pupils and staff must adhere to the policy and any incidents of possible misuse will need to be investigated. The school will include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.

- All staff must read and sign the Acceptable Use Policy.
- Parents should sign the their child's home-school agreement.
- The e-Safety Policy will be made available to all staff, governors, parents and visitors through the school website

It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. Please refer to the **Education for a Connected World Framework** for age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.

Responsibilities:

All members of staff and pupils are responsible for e-safety.

All Staff (including peripatetic, school governors and volunteers)

Staff are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. They must have a clear understanding of e-safety issues and the required actions from e-safety training sessions. Any e-safety issues must be reported to the headteacher or IT co-coordinator, as soon as the issue is detected. All staff must sign the staff Acceptable Use Policy (AUP) each year and abide by it each time they use school ICT equipment and systems, either in the school or elsewhere. Teaching Staff must educate pupils on e-safety through specific e-safety lessons and reinforcing this in the day to day use of ICT in the classroom.

Pupils

Pupils must participate in and gain an understanding of e-safety issues and the safe responses from e-safety lessons. They must comply with the pupil's Acceptable Use Policy (AUP) which pupils must abide by each time they use school ICT equipment and systems either in the school or elsewhere. They must report any e-safety issue

to the teacher, support staff or parent as soon as possible and take responsibility for their own actions using the internet and communications technologies.

IT Coordinator, Headteacher and IT Support Team

Their responsibility is to ensure that the best technological solutions are in place to ensure e-safety as well as possible, whilst still enabling pupils to use the internet effectively in their learning. They must ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition, any evidence of an e-safety breach must be secured and preserved. E-safety breaches must be dealt with from reporting through to resolution in conjunction with the headteacher. Work with governors to create, review and advise on e-safety and acceptable use policies and outside agencies including the police where appropriate. A log must be maintained of e safety issues. Lightspeed Systems which track student internet use to detect e-safety breaches must be monitored weekly by the headteacher.

How incidents are reported

All incidents are to be reported and logged on CPOMS as per the CPOMS training received by all members of staff.

Teaching and learning

Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

Pupils use the internet widely outside of school and will need to learn how to evaluate internet information and to take care of their own safety and security. The school internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements; Staff should guide pupils in on-line activities that will support the learning outcomes planned. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be expected to exercise the values of Belton C of E Primary School when working on the internet.

Evaluating Internet Content

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find

distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.

Users must act reasonably;

- Users must take responsibility for their network use. For all staff, flouting electronic use policy is regarded as a matter for discipline;
- Servers will be located securely and physical access restricted;
- The server operating system will be secured and kept up to date;
- Virus protection for the whole network will be installed and current;
- Fortingate Fire Wall will be utilised to protect systems and data
- Access by wireless devices must be pro-actively managed.
- The security of the school information systems will be reviewed regularly;
- Personal data sent over the internet should be encrypted or otherwise secured;
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail;
- The support team will review system capacity regularly

Emails:

Pupils may only use approved e-mail accounts on the school system. They must tell a teacher immediately if they receive offensive email. They must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.

The School Website

The contact details on the website should be the school address, e-mail and telephone number and the name of the staff member to whom to make contact. Personal information belonging to staff or pupils must not be published. E-mail addresses should be published carefully, to avoid spam harvesting. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should respect intellectual property rights and copyright.

Use of Images

Pupils' full names will not be used anywhere on the website or internet collaboration tools, particularly in association with photographs. Written permission from parents or carers will be obtained before images of pupils are electronically published.

Social Networking

The schools will block/filter access to social networking sites and newsgroups unless a specific use is approved. Pupils will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations. Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of friends,

specific interests and clubs etc. Pupils should be advised not to place personal photos on any social network space and should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school. Teachers should be advised not to run social network spaces for student use on a personal basis.

The use of webcams and video conferencing

At the present time video conferencing and web cams are not used in school and should there be a requirement to use them, this will only be done so after consultation with the head teacher.

Filtering

The school will work with IT Support, Schools Broadband and Lightspeed to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the computing coordinator or headteacher. This task requires both educational and technical experience. The IT support team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Weekly filtering reports will be scrutinised by the headteacher and any breaches reported immediately to the IT support team in the first instance.

Mobile phones will not be out during lesson time. The sending of abusive or inappropriate text messages is forbidden. Mobile phones are not permitted in school for pupils, if they are brought in they will have to be handed in at the start of the school day and collected at the end.

Protecting Personal Data

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

Internet Access

All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource. Access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Internet Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Leicestershire CC can accept liability for the material accessed, or any consequences resulting from internet use. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal

offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

E-Safety Complaints

- Complaints of internet misuse will be dealt with by the headteacher;
- All pupils will be taught to use the internet safely and about the role of CEOP to monitor and report abuse;
- Any complaint about staff misuse must be referred to the headteacher, unless it is the headteacher where complaints will be sent to the Chair of Governors;
- Parents and pupils will be informed of the complaints procedure;

Introducing and Communicating the Policy

Safety training will be given to all to raise the awareness and importance of safe and responsible internet use. Instruction in responsible and safe use should precede internet access.

Staff: All staff will be given the School e-Safety Policy and its application and importance explained. All staff will be trained in safeguarding procedures, including elements of E safety and the Prevent Duty. Staff should be made aware that internet traffic will be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents and Carers: Parents and carers' attention will be drawn to the school's e-Safety Policy through the website. The school will also organise E safety workshops to support parents' understanding of how to best safeguard their child against potential online dangers. School will liaise closely with the police and CEOPS to deliver this training. Internet issues will be handled sensitively, and parents will be advised accordingly.

Further Information

Further information on online safety in schools can be found in Annex C of Keeping Children Safe in Education (2016, DfE).

Appendix 1

The purpose of this E-safety appendix is to outline what measures the school takes to ensure that pupils can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion. The following are provided for the purpose of example only. Whenever a pupil or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the headteacher.

Pupils:

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in school e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to teacher; contact with parent; removal of internet access rights]

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to headteacher; contact with parent; removal of internet access rights for an extended period; exclusion]

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet

[Possible Sanctions: referred to headteacher; contact with parents; removal of equipment; removal of Internet access rights for an extended period; exclusion; referral to police]

Category D infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to headteacher; exclusion; removal of equipment; referral to police; LA e-safety officer]

Staff:

Category A (Misconduct)

- Excessive use of internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - referred to headteacher; Warning given.]

Category B (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software
- Any deliberate attempt to breach data protection or computer security rules
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the School into disrepute.
- [Sanction – Referred to headteacher and potential school disciplinary procedures; Referred to police; Referred to governors]

Child Pornography:

In the case of child pornography being found, the member of staff will be immediately suspended and the school disciplinary procedures implemented.

Other safeguarding actions:

● Remove the computer to a secure place to ensure that there is no further access to the PC or laptop.
● Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school.

- Identify the precise details of the material.
- Where appropriate, involve external agencies as part of these investigations.