E Safety Policy

Belton Lane Primary School

Approved by:	Jonathan Mason	**Date:**	January 2020
Last reviewed on:	September 2023		
Next review due by:	September 2025		

Linked Policies: Safeguarding Children Policy, Anti-Bullying

Policy, Peer on Peer Abuse Policy

Our e-Safety Policy and acceptable use guidance, build upon government legislation, to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. It has been agreed by the senior leadership team, staff and children and approved by governors.

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites;
- Learning Platforms and Virtual Learning Environments;
- Email and Instant Messaging;
- Chat Rooms and Social Networking (Facebook, What‟s App, Skype etc);
- Instant image sites (snapchat, instagram etc);
- Blogs and Wikis;
- Podcasting;
- Video Broadcasting;
- Music Downloading;
- Gaming;
- Online gaming;
- Mobile/ Smart phones with text, video and/ or web functionality;
- Other mobile devices with web functionality (e.g. tablets).

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. At Belton Lane Primary School, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) include both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named

e-Safety co-coordinator in our school is the Head teacher who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-coordinator to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection) and Childnet. Senior Management and Governors are updated by the Head / e-Safety coordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti bullying) policy and PHSE.

E-Safety skills development for staff:

- Our staff receive regular information and training on e-Safety issues in the form of updates at staff meetings, correspondence from co-ordinator;
- New staff receive information on the school's acceptable use policy as part of their induction;
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community;
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the school e-Safety messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used;
- The e-Safety policy will be introduced to the pupils at the start of each school year;
- E-Safety posters will be prominently displayed.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The school has a framework for teaching internet skills in ICT/ PHSE lessons;
- The school provides opportunities within a range of curriculum areas to teach about e-Safety including the dangers of social network sites;
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum;
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them;
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities;
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff

member, or an organisation such as Childline/ CEOP report abuse button.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety policy;
- Users will be provided with an individual network, email and Learning Platform log-in username;
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others;

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, and MIS systems including ensuring that passwords are not shared. Individual staff users must also make sure that workstations are not left unattended and are locked;

- In our school, all ICT password policies are the responsibility of Mr Charlesworth, all staff and pupils are expected to comply with the policies at all times.

  Data Security- The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the HT;
- Any data taken off the school premises must be encrypted Data and can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the school's learning platform is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school will provide supervised access to Internet resources (where reasonable) through the school's fixed & mobile internet technology;
- Staff will preview any recommended sites before use;
- Raw image searches are discouraged when working with pupils;
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research;
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources;
- All users must observe copyright of materials from electronic resources.

Infrastructure

- School internet access is controlled through Infotech's web filtering service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required;
- The school does not allow pupils access to internet logs;
- The school uses management control tools for controlling and monitoring workstations;
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-Safety co-ordinator;
- It is the responsibility of the school to ensure that Anti-virus protection is installed and kept up-to-date on all school machines;
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility nor the ICT co-coordinator's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media, it must be given to the teacher for a safety check first;
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher/ICT subject leader;

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school

  All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are;
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online;
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests);
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals;
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online;
- Our pupils are asked to report any incidents of bullying to the school;
- If children reveal any level of sexual and/or inappropriate knowledge accessed from the computer/Internet, the teacher must immediately report this to the designated Child Protection Officer;
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher;
- It is forbidden for any staff member to accept a current pupil or parent as a 'friend' on Facebook or any other social networking site – failure to comply will lead to disciplinary action.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use.
Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately. Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device;
- This technology may be used, however for educational purposes, as mutually agreed with the Head teacher. The device user, in this instance, must always ask the prior permission of the bill payer;
- Pupils are not allowed to bring personal mobile devices/phones to school without the permission of the class teacher and these phones should be stored at the school office at the start of the school day and collected at the end of the school day.
- The school is not responsible for the loss, damage or theft of any personal mobile device;
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed;
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community;
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used;
- In cases where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT to year 6 ARE or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed;
- Staff must use the official school e-mail system for work e-mails, ie outlook;

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business;
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses;
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper;
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account;
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes;
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission,
- virus checking attachments;
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform (the e-Safety co-ordinator and Headteacher) if they receive an offensive e-mail;

Use of Images

Taking of Images and Film Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment;
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device;
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site;
- in the school prospectus, newsletter and other printed publications that the school may produce for promotional purposes;
- recorded/ transmitted on a video or webcam;

- in display material that may be used in the school's communal areas;
- in display material that may be used in external areas, i.e. exhibition promoting the school;
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils" full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Head Teacher, office manager and ICT consultant teacher has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's equipment;
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher;
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network;
- The Headteacher has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Misuse and Infringements Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher. Incidents should be logged. Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator;
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart);
- Users are made aware of sanctions relating to misuse or misconduct. All staff are aware of the policy and the children have signed an acceptable use policy.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks. Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website) The school disseminates information to parents relating to e-Safety where appropriate in the form of:

- Information and celebration evenings
- Posters
- Website/ Learning Platform postings
- Newsletter items
- Learning platform training

Reviewing this Policy

- There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e- Safety that concerns them. This policy will be reviewed every 24 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Mason Headteacher/school e-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platforms and any related technologies for professional purposes or for uses deemed "reasonable" by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of Mr Mason
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not invite or accept a child or a parent as a 'friend' on Facebook or other social networking site. User Signature I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …… Date ……

Full Name……(printed)

Job title . . . . . .

Primary Pupil Acceptable Use Agreement / e-Safety Rules/Parental engagement with ICT

This is signed annually through Microsoft forms . See the following link

https://forms.office.com/Pages/DesignPageV2.aspx?subpage=design&FormId=AL71ys6-K0SOeFExC4rtLSmTOvMoZLhKlUd85SnLI75UMzA0NldTNzBCRDJSQU5NQ0FVU0dGQjVVQS4u&Token=cdeb3f75c97647c5be644a5c6fc9d85a