Burlington Junior School E-Safety Policy 2018

This policy was originally completed on 13.05.2010, reviewed 4.5.2011, 19.1.2012, 8.3.2013, 24.2.2015, 1.11.2017, 30.4.2018
This policy was approved by the governors on 8.3.2015
This policy is due for review no later than 1.11.2018

E-Safety Group
Alison Beckett (Headteacher)
Helen Gray (ICT Coordinator and eSafety coordinator and PSHE/SEAL Leader)
Julie Wright (ICT technician)
School Council to be involved in certain policy decisions.

We believe that eSafety is the responsibility of the whole community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Management Team
• Develop and promote an eSafety culture within the school community.
• Support the eSafety coordinator in their work.
• Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to eSafety effectively.
• Receive and regularly review eSafety incident logs and be aware of the procedure to be followed should an eSafety incident occur in school.
• Take ultimate responsibility for the eSafety of the school community.

Responsibilities of the eSafety Coordinator
• Promote an awareness and commitment to eSafety throughout the school.
• Be the first point of contact in school on all eSafety matters.
• Lead the school Digital Leaders group.
• Create and maintain eSafety policies and procedures.
• Develop an understanding of current eSafety issues, guidance and appropriate legislation.
• Ensure all members of staff receive an appropriate level of training in eSafety issues.
• Ensure that eSafety education is embedded across the new curriculum.
• Ensure that eSafety is promoted to parents and carers.
• Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
• Monitor and report on eSafety issues to the eSafety group and SMT as appropriate.
• Ensure an eSafety incident log is kept up-to-date (new log to be created and Mrs Beckett to store)

Responsibilities of Teachers and Support Staff
• Read, understand and help promote the school's eSafety policies and guidance.
• Read, understand and adhere to the new staff Acceptable Use Policy (AUP).
• Develop and maintain an awareness of current eSafety issues and guidance.
• Model safe and responsible behaviours in your own use of technology.
• Embed eSafety messages in learning activities where appropriate.
• Supervise pupils carefully when engaged in learning activities involving technology.
• Be aware of what to do if an eSafety incident occurs.
• Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilties of Technical Staff
• Read, understand, contribute to, and help promote the school's eSafety policies and guidance.
• Read, understand and adhere to the school staff AUP.
• Support the school in providing a safe technical infrastructure to support learning and teaching.
• Report any eSafety-related issues that come to your attention to the eSafety coordinator.
• Develop and maintain an awareness of current eSafety issues, legislation and guidance relevant to your work.
• Liaise with the local authority (LA) and others on technical issues.
• Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

• Read, understand and adhere to the school pupil AUP.
• Help and support the school in creating eSafety policies and practices and adhere to any policies and practices the school creates.
• Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
• Take responsibility for own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside of school.
• Respect the feelings, rights and values of others in your use of technology in school and at home.
• Understand what action should be taken if feeling worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if this is happening to someone you know.
• Discuss eSafety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

• Help and support your school in promoting eSafety.
• Read, understand and promote the school pupil AUP with your children.
• Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
• Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
• Discuss eSafety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
• Model safe and responsible behaviours in your own use of technology.
• Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

• Read, understand, contribute to and help promote the school's eSafety policies and guidance.
• Understand of the benefits and risks of the Internet and common technologies used by pupils.
• Understand how the school ICT infrastructure provides safe access to the Internet.
• Recognise how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
• Support the work of the eSafety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety activities.
• Ensure appropriate funding and resources are available for the school to implement their eSafety strategy.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

• We will provide a series of specific eSafety-related lessons in every Year group as part of the Computing, PSCHE and SEAL curriculum.
• We will celebrate and promote eSafety at a whole school level
• We will discuss, remind or raise relevant eSafety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
• We will remind pupils about their responsibilities through an end-user AUP which every pupil will sign and will be displayed throughout the school (classrooms and ICT suite).
• Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:
• include useful links and advice on eSafety regularly in newsletters, on our school website.

• to provide eSafety information in the school foyer area.

Managing ICT Systems and Access

• The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
• Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
• Servers, workstations and other hardware and software will be kept updated as appropriate.
• Virus protection will be installed on all appropriate hardware, and will be kept active and up-to-date.
• The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
• All users will agree to an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using the school ICT systems, and that such activity will be monitored and checked.
• Pupils will access the Internet using a class log-on. Internet access will be supervised by a member of staff.
• Members of staff will access the Internet using an individual log-on or the school log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school AUP at all times, including use of encrypted data storage as per AUP
• Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. head teacher, ICT coordinator, member of technical support
• The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
• The school will regularly audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate. We will regularly review our Internet access.

Filtering Internet access

• The school uses a filtered Internet service. The filtering is provided through East Riding of Yorkshire Council, along with the Smoothwall filter.
• If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafety coordinator.
• If users discover a website with potentially illegal content, this should be reported immediately to the eSafety coordinator. The school will report this to appropriate agencies including the filtering provider, LA, Child Exploitation and Online Protection (CEOP) or Internet Watch Foundation (IWF).
• The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Learning technologies in school

Using email and messaging facilities

• Staff and pupils should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system can be monitored and checked.
• Pupils will be allocated a group e-mail account for their use in school. Classes will be allocated an individual e-mail account for use by pupils within that class, under supervision of the class teacher.
• Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
• Staff and pupils are not permitted to access personal e-mail accounts during school.
• Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
• Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

• We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
• Digital images, video and sound will only be created using equipment provided by the school.
• Staff and pupils will follow the school policy on the use of photographs, digital images and video.
• In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used

either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.
• If pupils are involved, relevant parental permission will also be sought before resources are published online.

Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

We use blogs to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.
• Blogging and other publishing of online content by pupils will take place within the school's website. Pupils will not be allowed to post or create content on sites where members of the public have access unless they are supervised by a member of the teaching staff.
• Any public blogs run by staff on behalf of the school will be hosted on the learning platform or the school website and postings should be approved by the headteacher, eSafety coordinator or class teacher before publishing.
• Year 5 and 6 pupils will have the opportunity to create a social networking page to sit within the school's website. This will be introduced as part of their eSafety curriculum and will be monitored by class teachers.
• Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

Using video conferencing and other online video meetings

We may use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner.
• All video conferencing activities will be supervised by a suitable member of staff.
• Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.
• Video conferencing equipment will be switched off and secured when not in use.
• Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
• Video conferencing should not take place off school premises without the permission of the head teacher.
• Parental permission will be sought before taking part in video conferences.
• Permission will be sought from all participants before a video conference is recorded.
• Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

Using mobile phones

• Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.
• If pupils bring mobile phones to school, they will be handed in at the school office at the start of the day.

Using new technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafety point of view.
• We will regularly amend the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafety risk.

Protecting personal data

• We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
• Staff will ensure they properly log-off from a computer terminal after accessing personal data.
• Staff will not remove personal or sensitive data from the school premises without permission from the head teacher, and without ensuring such data is kept secure.
Staff will use encrypted data storage for all school work on and off site.

The school website and other online content published by the school

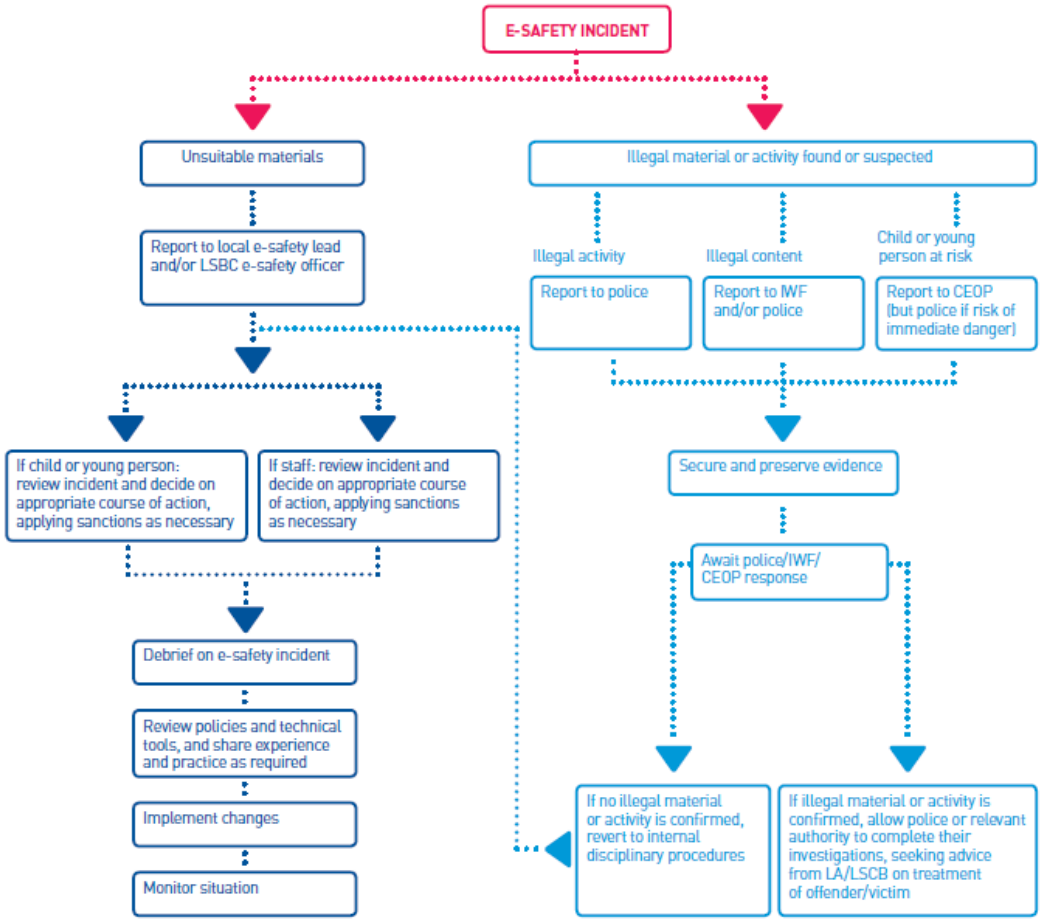
• The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.
• A generic contact e-mail address will be used for all enquiries received through the school website.

• All content included on the school website will be approved by the head teacher, eSafety coordinator or class teachers before publication.
• The content of the website will be composed in such a way that individual pupils cannot be clearly identified (names and photographs will not be displayed together)
• Staff and pupils should not post school-related content on any external website without seeking permission first.

Dealing with eSafety incidents

• Staff will log eSafety incidents.
• The eSafety coordinator or the Head teacher will be the first point of contact in school on all eSafety matters.

Flowchart for responding to e-safety incidents



(reproduced from 'AUPs in Context: Establishing Safe and Responsible Online Behaviours', © copyright Becta 2009)

Examples of eSafety incidents

- accessing illegal content deliberately
- accessing inappropriate content deliberately
- accessing illegal content accidentally and failing to report this
- accessing inappropriate content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school
- accessing social networking sites, chat sites, instant messaging accounts or personal email where not allowed
- accessing other non-educational websites (e.g. gaming or shopping websites) during lesson time
- downloading or uploading files where not allowed
- sharing your username and password with others
- accessing school ICT systems with someone else's username and password
- opening, altering, deleting or otherwise accessing files or data belonging to someone else
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature
- attempting to circumvent school filtering, monitoring or other security systems
- sending messages, or creating content, that could bring the school into disrepute
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)

Examples of additional eSafety incidents where staff could be involved would include:

- transferring personal data insecurely
- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites)
- failure to abide by copyright of licencing agreements (for instance, using online resources in lessons where permission is not given)

Acceptable Use Policy for Pupils

You can use the computers and other devices in school to access the Internet to help you with your learning. These rules will help make sure the Internet is a safe and fun place for everyone in school. You will need to agree to follow these rules whenever you use ICT at school.

- I will ask permission from a member of staff before using the internet.
- I will only use the computers and other devices for school work and homework.
- I will not access files that belong to other people.
- I will only use equipment or files I bring from home, such as my mobile phone or files on a USB stick, if the school lets me, and for activities the school agrees to.
- I will only send messages to people I know, or my teacher has approved, as part of my lesson.
- The messages I send, and the work I do, will be polite and responsible, and will not contain anything that might upset someone else.
- I will only open attachments in messages I receive, or download a file, if I trust the person who sent it or the website it is from, and I've checked with my teacher that it is safe.
- I will keep my username and password safe by not telling anyone else.
- I will not change any settings on the computers and other devices I use at school.
- I will not install or delete any software on the computers and other devices I use at school.
- I will not give away any of my personal information, or the personal information of people I know, over the Internet. This includes my full name, address, phone numbers, photographs and videos of me and my friends, or the name of my school unless my teacher has checked it is safe.
- If something happens whilst using a computer or school device, and I am not sure what I should do next, I will ask a member of staff to help me.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- I understand that the school may check my computer files, the Internet sites I visit, the messages I send and anything else I do to make sure I am keeping myself and others safe.
- I understand that if I do not follow these rules and other guidance from the school as best as I can then I may not be allowed to use the Internet or any of the school's ICT equipment.

Acceptable Use Policy for Staff and other adults in school

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using the ICT systems provided. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school ICT equipment at other locations such as your home.

- Any use of school ICT systems will be for professional purposes.
- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the ICT systems. You should not allow an unauthorised person to access the school ICT systems, e.g. by logging in for them.
- Any online activity should not harass, harm, offend or insult other users.
- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow your school's procedure and report this immediately.
- You should not download or install any hardware or software without permission. If you have responsibility for installing software you should be confident it is adequately licensed and appropriate for educational use.
- Ensure that any files on removable media (e.g. USB drives, CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Headteacher.
- Any electronic communications should be related to schoolwork only, and should be through school e-mail addresses or other school systems. It is not acceptable to contact pupils using personal equipment or personal contact details, including your own mobile phone or through your personal social network profiles.
- Any online activity, including messages sent and posts made on websites, and including activity outside of school, should not bring your professional role or the name of the school into disrepute.
- Any still or video images of pupils and staff should be for professional purposes only. They should be taken on school equipment, and stored and used onsite. Such images should not be taken off-site without permission and valid reason.
- You will not give out your personal details, or the personal details of other users, to pupils or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents.
- You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately.
- Personal or sensitive information should only be taken off-site if agreed with the Headteacher, and steps should be taken to ensure such data is secure.
- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.
- You should support and promote the school eSafety Policy, and promote and model safe and responsible behaviour in pupils when using ICT to support learning and teaching

Finally:

You understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies you may be subject to disciplinary action in line with the school's established disciplinary procedures.

Image Consent Form 2018

At Burlington Junior School we take the issue of child safety very seriously, and this includes the use of images of pupils. Publishing images of pupils in local newspapers, school publications and on the school website can be motivating for the pupils involved, and provide a good opportunity to promote the work of the school. However, schools have a duty of care towards pupils, which means that pupils will remain un-identifiable by full name except in local newspaper reports that may accompany photographs.

We ask that parents consent to the school taking and using photographs, video footage and images of their children for use in the school prospectus, educational purposes within school, website, learning platform or other publications**. We undertake to never include the full name of the pupil alongside an image in our published material, learning platform or website.**

When parents, friends, pupils, ex pupils and relatives are invited to school events, many will want to record the occasion for their personal use. The school believes that this is reasonable and will generally allow the use of cameras and video recorders unless we receive an objection in writing beforehand. From time to time the school may make DVD's of school events for sale to the school community. We ask that your consent for this may be assumed unless we have received a written objection beforehand.

The school arranges for a specialist company to visit in order to take individual and class photographs. This company operates under a strict code of conduct and any unwanted photographs will be destroyed. All children are included in these photographs unless the school receives written objection beforehand.

Although the school will always employ a common sense approach to this issue, whereby we uphold the welfare of the children of the school, to comply with aspects of the Data Protection Act 1998 we need to ask you to complete and return this form to the school office.

I consent to photographs, video footage and digital images of the child named below, appearing in Burlington Junior School's printed publications or on the school website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in the promotional activities of the school.

Name of child: .....

Name of parent or guardian: .....

Address: .....

Signature: ..... **Date:** .....