Burlington Infants School

e-Safety Policy

We believe that e-Safety 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 Headteacher and Senior Management Team

- Develop and promote an e-Safety culture within the school community.
- Support the Computing Subject Leader in their work.
- Make appropriate resources, training and support available to the school community.
- Ensure all members of staff receive an appropriate level of training in e-Safety issues.
- Receive and review e-Safety incidents and be aware of the procedure to be followed should an e-Safety incident occur in school.
- Ensure an e-Safety incident log is kept up-to-date.
- Take ultimate responsibility for the e-safety of the school community

Responsibilities of the Computing and e-Safety Subject Leader

- Promote an awareness and commitment to e-Safety throughout the school.
- Develop an understanding of current e-Safety issues, guidance and appropriate legislation.
- Create and maintain e-Safety policies and procedures.
- Be the first point of contact in school for general e-Safety matters.
- Ensure that e-Safety education is embedded across the curriculum.
- Ensure that e-Safety is promoted to pupils, parents and carers.
- Monitor and report on e-Safety issues to the Headteacher and SMT as appropriate.

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school e-Safety policies and guidance.
- Read, understand and adhere to the school's Acceptable Use Policy for Staff (all staff should read, sign and date policy and give copy to Headteacher).
- Develop and maintain an awareness of current e-Safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed e-Safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an e-Safety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Technical Staff

- Read, understand, contribute to, and help promote the school e-Safety policies and guidance.
- Read, understand and adhere to the school's 'Acceptable Use Policy for Staff' (AUP).
- Support the school in providing a safe technical infrastructure for teaching and learning.
- Report any e-Safety related issues or concerns to the Headteacher.
- Develop and maintain an awareness of current e-Safety issues, legislation and guidance relevant to 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 (Age Appropriate)

- Agree to follow the 'Acceptable Use Policy for Pupils.'
- Take responsibility for learning about the benefits and risks of using the internet and other technologies at school and at home.
- Take responsibility for your own and each others' safe and responsible use of ICT in school and at home.
- Understand what action you should take if you feel worried, uncomfortable or at risk of using technology at home or in school.
- Discuss e-Safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support school in promoting e-Safety.
- Read, understand and promote the school's 'Acceptable Use Policy for Pupils' 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 e-Safety 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 behaviour 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 e-Safety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and technologies used by pupils.
- Develop an overview of how the school provides safe access to the Internet.
- Develop an overview of 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 school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to take part in e-Safety activities.
- Ensure appropriate funding and resources are available for the school to implement their e-Safety strategy.

Learning and Teaching

We believe that the key to developing safe and responsible behaviour 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 benefit safely from the opportunities the Internet brings.

- We will provide specific e-Safety-related lessons in every year group as part of the Computing and PHSCE curriculum.
- We will celebrate and promote e-Safety through assemblies and whole-school activities, including promoting Safer Internet Week each year.
- We will discuss, remind or raise relevant e-Safety messages with pupils routinely, in an age appropriate way, wherever suitable opportunities arise during all lessons.
- We will remind pupils about their responsibilities through the school's 'Acceptable Use Policy for Pupils,' which will be taught as part of the PHSCE and Computing Curriculums.
- 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:

- Arrange e-Safety talks and training, linking with the Junior School when possible.
- Include useful links and advice on e-Safety regularly in newsletters and on our school website.
- Include a section on e-Safety in the School Prospectus.

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 through the following:

- 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 is 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.
- All users will agree to an 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.
- All pupils are logged on as pupils in the Computing Suite only allowing them access to certain areas. Internet access will be supervised by a member of staff.
- Members of staff will access their internet through their own individual log on.
- Support staff will be provided with a separate log on.

- Members of staff 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.
- 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 and 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 uses a filtered internet service, provided by the Local Authority.
- If users discover a website with inappropriate content, this should be reported to the Headteacher immediately
- The school will regularly audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate. We will regularly review our Internet access.

Using E-mail

- Staff have their own e-mail accounts which they use at home and at work. All staff can also be contacted through the school email address burlington.infants@eastriding.gov.uk

Using Digital Images, Videos and Sound

- Digital images, video and sound will only be created using equipment provided by the school
- Staff will follow the school Acceptable Use Policy on the use of photographs, videos, mobile phones and social networking sites

Using mobile phones

- Staff will not be expected to use personal mobile phones in any situation around children in the school or classroom.
- Staff will not be expected to use their personal mobile phone in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.
- Staff can, however, use personal mobile phones on school trips to keep in touch with school and for dealing with any emergencies

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 e-Safety point of view.
- We will regularly amend the e-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an e-Safety 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.

The school website

- The school website will not include the personal details, including individual e-mail addresses or full names of staff or pupils.
- All content included on the school website will be approved by the Head teacher, e-Safety 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.
- Permission from parents will be sought in writing before any photographs of children are used on the school website.
- Staff and pupils should not post school-related content on any other external website without seeking permission first.

Dealing with E-Safety incidents

- The Head teacher will be the first point of contact in school on all e-Safety incidents.
- The flow chart for responding to e-Safety incidents will be followed (see Appendix A).
- All e-Safety incidents will be logged.

Burlington Infants School

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 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 e.g. learning platforms. 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.

Signed: …… Print Name: …… Date: ……

Burlington Infant School
Acceptable Use Policy for Pupils

We can use the Internet safely to help us learn.

We know to ask a grown up for help.

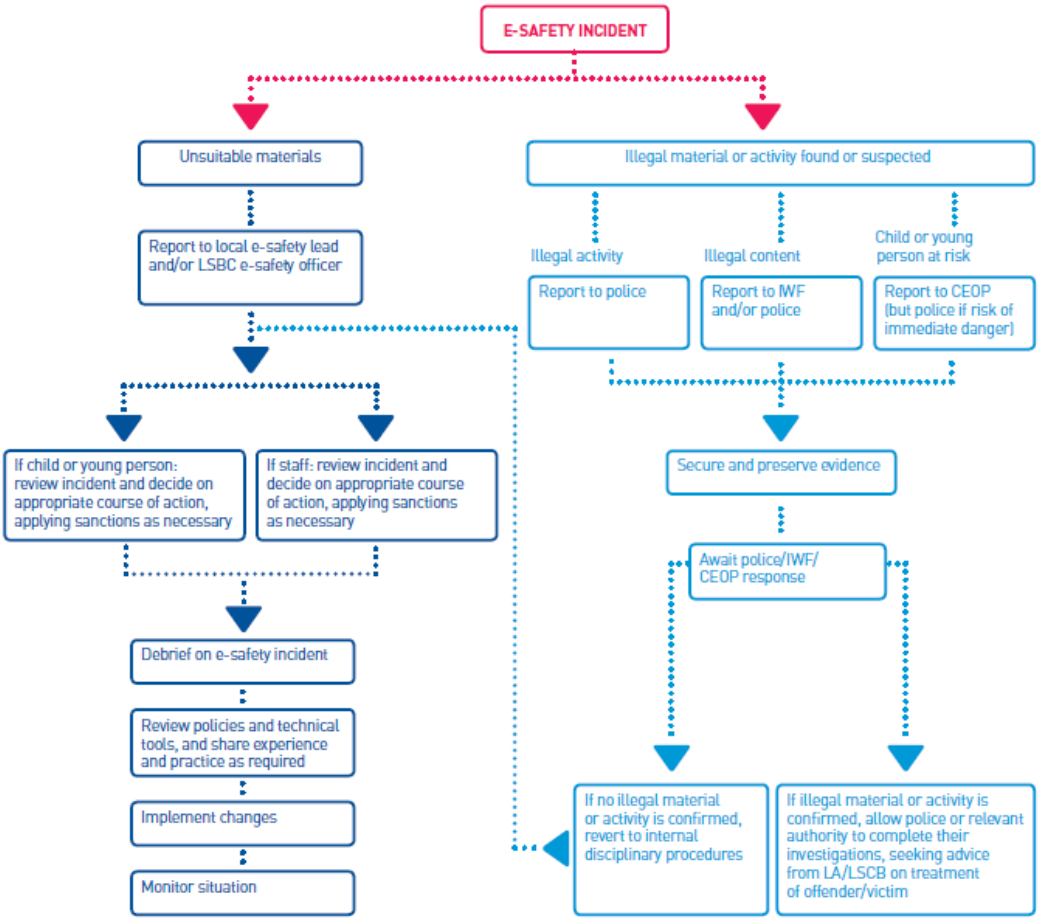
If we see something we do not like we know what to do.

We know that it is important to follow the ICT Suite rules.

<u>Our Top Tips for Using the Internet Safely</u>

- Never tell anyone your age
- Never tell anyone where you live
- Never have your photograph as your profile picture
- Your password should be made of numbers and letters
- Never tell anyone your password

Appendix A 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 e-Safety 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)