Bellfield Infant School

E-Safety Policy

Aims

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 business administration systems. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

All internet use is monitored by Policy Central. Policy Central is a software product used by many schools that monitors internet usage and can detect potential misuse, for example; violence, pornography and abusive language. Screen shots and key strokes are taken regularly and only nominated school staff monitors the generated data.

All staff and other adults using the school's computer systems sign an **Acceptable Use Statement** and are familiar with the guidelines detailed in Appendices 1-4. Students working on placement in the school will also sign an Acceptable Use Statement prior to their placement and it is the class teacher's responsibility to ensure a copy is signed. These will be stored by the School's Office Manager, who will be responsible for the maintenance of the statements.

All staff and other adults using the school's computers are issued with guidelines (Appendices 1-4) regarding the safe use of the Internet for both staff and pupils and safe use of e-mail, at the beginning of each Academic year, and must make themselves familiar with the content. Copies of the guidelines are stored in the ICT Policy folder kept in the school's staff room. It is the class teacher's responsibility to ensure that students working in their class will also be given a copy prior to their placement.

Pupil guidelines are communicated to the children to ensure their understanding at the beginning of each Academic year. The wording of the statements is adapted in order to enable the children to gain understanding at their level. Children are made aware of safety issues, including the appropriate use of e-mail and social networking sites. They are also reminded regularly throughout the year by the class teacher. Children are advised to tell the teacher or an adult should they receive any inappropriate messaging when using the internet.

School's Website and Blog

The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published. Website photographs that include pupils are selected carefully. Pupils' full names are not used anywhere on the website, particularly associated with photographs. Written permission from parents is sought as part of the school's admission process, before photographs of pupils are published on the

school website. Where we have been informed that a child is subject to a court order, we will never use their image.
The head teacher takes overall editorial responsibility and ensures content is accurate and appropriate. The Website complies with the school's guidelines for publications. The copyright of all material is held by the school, or is attributed to the owner where permission to reproduce has been obtained.

Social networks and online communications

Staff are advised that all private-life information becomes public once shared on a social networking site. The reputation of the school must not be brought into disrepute by anything posted on a social networking site by a member of staff. No parent or pupil should be accepted as a "friend". Publishing anything that brings the school into disrepute can lead to disciplinary action or dismissal. Permission must be sought from other persons before posting photos of them on a social networking site.

Mobile Phones

All mobile phones brought on site should be PIN protected in case of loss or theft. Staff must not use their own personal devices to take and store images of pupils. School cameras must be used always. All photos should be stored on the school network. Personal devices should be locked away when staff are working with children.

Physical Environment and Security

Anti-virus software is installed on all computers and updated regularly by the ICT Technician. Central filtering is provided and managed by Link2ICT and all incidents will be recorded in the E-Safety log for audit purposes. The school uses Policy Central Enterprise on all school-owned equipment to ensure compliance with the Acceptable Use policy. No computers are allowed to be used in school that link to the internet with modems via telephone lines, using other Service Providers, thereby by-passing the filtered services. A risk assessment is carried out before any new technology is allowed.

Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998. Data should not be kept longer than necessary. "Restricted" paperwork should be labelled and not left accessible to others. Staff should only store data for the purposes of tracking and analysis on the school network. Staff should be aware that should they lose data they are personally liable for this. This Policy has been written, building on the Birmingham Grid for Learning (BGfL) policy and government guidance. It has been agreed by the senior management and approved by governors and will be reviewed annually.

Written by: GE Simm
Date: Spring 2018
Ratified by Governors:
Date of next review: Spring 2020

Bellfield Infant (NC) School

(E Safety Policy Appendix 1)

E-Safety Staff Guidelines

Bellfield Infant School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and communication technologies. We are aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end the school aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

E-mail

Staff are given a school e-mail address and understand that this should be used for all professional communication. Under no circumstances must staff access private e-mail addresses on school equipment.

Social networks and online communications

Staff are advised that;

- All private-life information becomes public once shared on a social networking site.
- The reputation of the school must not be brought into disrepute by anything posted on a social networking site by a member of staff.
- Permission must be sought from the other person before posting a photo of them on a social networking site.

Mobile Phones

All mobile phones brought on site should be PIN protected in case of loss or theft.
Personal devices should be locked away when staff are working with children.
Staff must not use their own personal devices to take and store images of pupils.

Digital Media

Photographs uploaded to the school's website must not focus on any pupil, but be focussed on the activity. No front view or whole body view of a pupil should be posted to the website or used in other media such as Newsletters etc. without parental permission. All photos should be stored on the school network. School cameras/recording devices must be used always.

Bellfield Infant (NC) School

(E Safety Policy Appendix 2)

E-Safety Staff Guidelines – Use of E-Mail

The following guidelines will help implement the safe use of e-mail.

1. Staff must use their business and not their private e-mail address; a business e-mail account will be allocated to them by the ICT Co-ordinator/Technician.

2. If Staff receives abusive or offensive e-mails they must not reply to them and should report such occurrences to the ICT Co-ordinator who in turn will notify the necessary persons within Link2ICT.

3. Staff should not give details in e-mails, or in any other way on the Internet, that could identify their home address or phone number/mobile number.

4. Sensitive or confidential information must not be sent by e-mail over the Internet.

5. Staff must be aware that e-mails sent and received via school computers may be inspected at any time.

6. Staff should be aware that e-mails from the school present an image of the school to recipients and therefore should not contain anything that would cause offence or present the school or user in a bad light.

Examples of good practice when using email.
As the use of email continues to grow, there is a need to identify good practice. The suggestions below are a few examples of good practice.

Ensure teachers are aware of who is responsible for monitoring the use of email.

Do not forward chain letters to anyone else, but report them to the appropriate person (ICT Co-ordinator).

Know how to deal with and avoid receiving junk mail and unsolicited mail.

Do not impersonate anyone else using e-mail.

Do not use e-mail to send comments or information that is defamatory or libellous, or use e-mail as a means of harassment, intimidation or annoyance to anyone else. (The sender of an e-mail should only send messages the contents of which they would be happy to be received or have read out in court. E-mail messages are admissible as evidence). Do not reply to pestering, offensive or suggestive e-mails - these should be reported to the ICT Co-ordinator.

There is a growing instance of computer viruses being sent by email, often innocently. If you think you have received a virus, delete the email ***without opening*** it and report it to the ICT Co-ordinator.

Bellfield Infant School (NC)

(E Safety Policy Appendix 3)

E-Safety Staff Guidelines – Use of the Internet

The following guidelines will help implement the safe use of the Internet.

1. All staff and adults in schools who will at some time be responsible for supervising pupil use of the Internet, should be trained or experienced in its use and be aware of the issues surrounding use in schools.

2. All school staff must be aware that there is a considerable amount of material on the Internet that is unsuitable for pupils. This includes pornographic, racist, extremist, political, drug related information as well as information which is deliberately misleading or incorrect.

3. Schools have a duty of care and must take all reasonable steps to protect pupils against deliberate or accidental access to such material. In practice this is likely to be through the use of an electronic filtering mechanism supported by careful supervision of Internet use by pupils. All computers connected to the Birmingham Grid for Learning, benefit from sophisticated filtering software. However, staff must be aware that no filtering system will be 100% secure. Undesirable sites should be reported to the ICT Co-ordinator and the helpdesk at Link2ICT for addition to the filtered list.

4. Supervision of pupils using the Internet by staff/adults who are aware of the Internet and the issues surrounding its use is essential. Staff should know what they are looking at and how to trace the history of website access during a particular session.

5. There are systems to monitor the use of the Internet made from individual computers. Staff and pupils need to be aware of this activity.

6. Schools may consider the use of an Intranet to store Internet information for local use while restricting live access to the Internet.

7. It may be appropriate to restrict access to the Internet from particular computers or for particular users. This is possible using a password or network access control function. Contact the Helpdesk at Link2ICT for assistance if needed.

8. Pupils should be encouraged to develop an understanding of what is and what is not appropriate material and should be encouraged to inform the teacher should such material be found.

9. Staff, pupils and members of the community coming into school to use the ICT facilities, should sign an 'Acceptable Use Statement'.

10. To help teachers and schools educate children on staying safe on the internet, Staff may consider using these materials:

- Internet Proficiency Scheme - **http://www.safety.ngfl.gov.uk/schools**
- Child exploitation and on-line protection centre- **http://www.ceop.gov.uk/**
- The Internet Watch foundation - **http://www.iwf.org.uk/**

Bellfield Infant School (NC)

(E Safety Policy Appendix 4)

Acceptable Use Statement for Pupils

Pupil guidelines for using the Internet

1. Never give your home address, phone number, mobile number or a picture of yourself or friend/s on the Internet.
2. If you have a password, do not tell or give your password to anyone who does not need to know it. Check with your teacher or supervising adult that it is okay to give this information before doing so.
3. Never access any area on the Internet other than that indicated by the teacher or supervising adult.
4. Always tell your teacher or supervising adult if you receive messages suggesting that you should meet somebody you do not know.
5. Never send or respond to nasty, suggestive or rude messages.
6. Always tell your teacher if you see inappropriate language or nasty pictures on the Internet.
7. If pupils encounter material they feel is not appropriate, they should notify a member of staff or supervising adult immediately.

Pupil guidelines for use of e-mail accounts.

- Pupils in Year 2 at Bellfield Infant School will be provided with an e-mail account in an in-house secure intranet environment and will be taught the appropriate use of e-mailing.
- Pupils may only use the approved e-mail accounts on the school 'Knowledge Box' intranet system.
- Pupils must immediately tell a teacher if they receive an inappropriate e-mail.
- Pupils must not send inappropriate e-mails to others.
- Pupils must not use inappropriate words in their e-mails.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.

Acceptable Use Agreement

I am aware of the rules for using the internet and e-mailing and promise to follow them at all times.   I understand that misuse of school computer equipment is a serious offence.

Full name (Printed) ____

Signed _________________________________   Date ___________

Class Teacher _____________________________   Date ___________

Bellfield Infant School (NC)

Acceptable Use Statement – For staff and adult users

The computer systems within school and the Children's Centre are made available to students, staff, and other adults to further their education and to enhance professional activities including teaching, research, administration and management. The school's E Safety Policy has been drawn up to protect

Staff and other adults wishing to use the school computer systems, email or Internet should sign a copy of this **Acceptable Use Statement**, which should be countersigned by the Head teacher and returned to the School's Office Manager.

- All Internet activity should be appropriate to the student's education;
- Access to the network should only be made via the authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Users are forbidden to use private e-mail addresses and MUST use the e-mail address allocated to them by the ICT Technician.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Use of the internet for personal shopping, banking etc. is forbidden.
- Access to Gaming sites or any social networking sites is forbidden.
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- If you are linked up to any site on the internet which you feel is inappropriate, report it in writing as soon as possible to the ICT Co-ordinator. Retain a copy of the report.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden. This also needs to be considered when using 'social network sites' outside of school with reference to Teacher Standard's (to maintain high standards of ethics and behaviour, within and outside school).
- E-Safety Staff guidelines will be adhered to at all times.

Misuse of school computer equipment, email or the Internet are serious offences. Link 2ICT has a contractual obligation to monitor the use of the e-mail and Internet services provided as part of the BGfL, this information may be recorded and may be used in disciplinary procedures if necessary. Link2ICT, BCC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. **Acceptable Use Agreement.**

I have read the statement above and agree to abide by the terms. I shall adhere to the Staff E-Safety guidelines. I understand that misuse of school computer systems, email or the Internet are serious offences. I also acknowledge that a professional standard must be maintained on public sites and failure to do so could lead to disciplinary procedures, up to and including dismissal.

Full name (Printed) ____

Signed _______________________________ Date _________

Head Teacher __________________________ Date _________