Basildon CE Primary School

E-safety Policy

Created:June 2015
Approved: December 2016
Review due: December 2017
Author: P. Field

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Basildon Primary School, we recognise that learning is a lifelong process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. E-safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

This policy has been developed to ensure that all adults in Basildon Primary School are working together to safeguard and promote the welfare of children. E-Safety is a safeguarding issue and not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1. Physical Safety:

1. All electrical equipment in the school is tested annually to ensure that it is safe to use.
2. All the projectors in our school have maximum light levels below the government's health and safety guidance of 1,500 ANSI lumens.
3. Workstations are cleaned and sanitised regularly.
4. Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks.

2. Personal Safety:

1. Access to social networking sites is not permitted within school.
2. Pupils are taught the importance of personal safety when using the internet both inside and outside of school.
3. There are clear procedures to follow in the event of children or adults encountering inappropriate material or websites. All reports of unsuitable content will be referred to the appropriate authority for blocking or removal.

4. In addition to the general filtering applied in the WAN, the school manages its own local filtering. All authorised staff (currently the headteacher and school business manager) are expected to maintain an appropriate level of safety and suitability.

3. Network Safety:

- All users need to log on using a username and password.
- Each user is given an allocation of disk space for the storage of their work.
- Access to other users "My documents" areas are restricted by the network.
- On the network there are "shared resource" areas where many different groups of users can save work so that it is available to others.
- The network software prevents changes being made to computer settings.
- Only the network administrators are permitted to install software on to computers.
- All users of the network can be monitored remotely by the network administrators.

4. Internet Safety:

1. All pupils and staff are expected to follow the school's Internet Usage Policy which should be read in conjunction with this policy.
2. When using a network workstation all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses which are considered to be unacceptable. However, no system is 100% safe and we expect users to behave responsibly.
3. Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. *However, it is expected that all pupils will follow the principles of this policy in any school related internet activity*.

5. Email Safety:

1. Pupils have an identity within the school's Google domain. Emails are only used as part of our collaboration project with schools in the JDO project. These schools have been whitelisted and all communication is supervised and forms part of our wider curriculum.
2. Some pupils will have their own webmail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore we do not permit the use of personalised email accounts by pupils at school or at home for school purposes.

6. Digital Images:

1. Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website. On the website we never state a child's full name with their image.
2. Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff.

7. E-Bullying:

The school takes bullying very seriously and has robust procedures for identifying and dealing with it. E-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. E-Bullying is included in our regular e-safety education programme. Whilst most instances will occur outside of school, we are prepared to work with parents to deal with any issues they may bring to our attention.

8. **Mobile Phones:**

Pupils are not permitted to have mobile phones upon their person in school. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. In this event, the mobile device should be handed in to the class teacher upon arrival and it will be stored securely during the day.

9. Other technologies:

1. **Podcasting** – Some pupils will be given opportunities to create oral recordings. Some of these recordings may be made available as podcasts through the Internet so that they can be shared with interested members of the school community.
2. **YouTube** – the school aims to produce a variety of videos for use on the school's YouTube Channel. These do include children sometimes. All videos are monitored by the channel administrator who ensures that all videos are appropriate and do not create any danger to our pupils or staff.

10. Copyright:

Though there are lots of 'free to use' resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology – further guidance can be sought from the school business manager?.

It is important to know what work is original and when chunks of text have been copied from other sources such as the Internet

11. Data Protection Act:

The Data Protection Act 1998 gives you the right to access information held about you or your child by the school. The school has the right to charge for supplying this information. Further information on the Data Protection Act can be obtained from the Department of Constitutional Affairs – www.justice.gov.uk