



## Introduction

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' that applies to everyone working with children.

Although the children at our school are young, we expect that they will be using these technologies on a regular basis. In the classroom, they use iPads and computers and they complete homework through online platforms such as Education City. Undoubtedly they will have access to a range of other technologies in their home and wider environment. This document aims to find a balance between controlling access to the Internet and technology, setting rules and boundaries, and educating students and staff about responsible use.

Children and staff cannot be completely prevented from being exposed to risks both on and offline. We aim to empower and educate children so that they are equipped with the skills to make safe and responsible decisions, as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

In order to support these aims, the school has developed this e-Safety policy, and taken the following steps:

- The school has appointed an e-Safety coordinator.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy has been developed particularly for the needs of our school, building on the DCC e-Safety Policy and government guidance.
- The School has appointed a member of the Governing Body to take lead responsibility for e-Safety

## Use of the Internet in School

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 functions.

### Using the Internet to Enhance Learning

Internet use is part of the statutory curriculum and is a necessary tool for learning. The school has a duty to provide students with quality Internet access as part of their learning experience. There are a wide range of benefits of using the Internet in education, including:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with KCC and DfE;
- access to learning wherever and whenever convenient.

The provision of Internet access at school allows staff to guide pupils to make use of these resources, at a level appropriate to their age.

### Evaluating Internet Content

A wealth of information is available on the Internet, providing a wide selection of resources to support teaching and learning. However there is also material of dubious credentials, both in the quality of materials, and in the copyright status of materials. At our school, due to the age of pupils, they will only access the Internet under direct adult supervision. Pupils will use age-appropriate tools to research Internet content. Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.

When staff make use of Internet-derived materials in their teaching, they will use their professional judgement to ensure the credibility of the material, and furthermore they will ensure that this use complies with copyright law.

## Management of Information Systems

### ICT Security

ICT security is a complex issue that cannot be dealt with adequately within this document. The school follows guidance from IT specialists on the implementation of ICT security measures. This includes physical measures (such as etching and warning stickers, and a building alarm systems) and software measures (such as logging of usage, encryption of data, anti-virus and firewall protection, and separate accounts for all users).

The school will ensure that:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media will not used without specific permission **and** an anti-virus / malware scan.
- Unapproved software will not be allowed on school computers.

### Email

Policy on staff email use is covered in a separate policy document, *School Staff IT Acceptable Use*.

Pupils will not be given individual email accounts through school. In some instances, a whole-class or group email address may be set up for particular projects (for example, when collaborating with a partner school), but access to these accounts will be controlled by staff members. Pupils may compose messages to be sent through such accounts, but any such correspondence will be moderated and only sent by staff members. Similarly, staff members will review any messages received in such accounts, and only display the contents to pupils if it is deemed appropriate.

### The School Web Site

The school web site is a valuable resource for the school community, providing a repository for documents such as newsletters, a first point of contact for information regarding the school (including the school prospectus), and an opportunity to showcase the school. It is also a very public view of the school, and as such, great care must be taken to avoid disclosing personal information.

- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Access to private areas of the web site will be carefully controlled, with accounts and passwords that are covered by the separate *Acceptable Use of IT Policy*.

#### **The Use of Pupils' Images, Videos or Work on the School Web Site**

- Images or videos that include pupils will be selected carefully to provide minimal opportunity to reuse images of individually recognisable pupils. This could be achieved for example by using small, low resolution images, images which do not capture the face, or group shots.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils' work can only be published with parent's permission.

#### **Social Networking, Social Media, and Personal Publishing**

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chat rooms, instant messenger and many others. There are significant risks in sharing personal information on such platforms, as there is no way of verifying the identity of other users, or of controlling the sharing of such information. Even when such information is shared with only a restricted audience, it is sometimes possible that it can be "leaked" to a wider audience.

Policy on staff use of such platforms is covered in a separate policy document, *School Staff IT Acceptable Use*.

Due to these risks mentioned above, and the young age of our pupils, the school recommends that they do not use these platforms. Most such platforms in any case have a minimum age requirement that is not met by our pupils, but even when it is legally permissible for them to use platforms of these types, we urge parents to consider carefully the risks that would be associated with these platforms.

The school will control access to social media and social networking sites. Pupils will be advised never to give out personal details of any kind that may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

#### **Internet Filtering**

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with DCC to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.

- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

### **Videoconferencing**

Videoconferencing (including use of products such as Skype or Flashmeeting) enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education. For example, pupils could engage in group work with children at a twinned school, or speak to an educational expert from a museum or zoo.

- Access to videoconferencing equipment and software will be carefully controlled, and only used for specific educational purposes.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.
- If a videoconference lesson is recorded, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.

### **Emerging Technologies**

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. Until such a risk assessment is undertaken, these technologies should not be used in school.

### **Data Protection**

The school takes its data protection responsibilities seriously. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

### **Authorised Access of School Internet**

- All staff will read and sign the *School Staff IT Acceptable Use Policy* before using any school ICT resources, including the Internet.
- Pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.

### **Risks, Incidents of Concern, and Complaints Related to Internet Use**

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected

nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor DCC can accept liability for the material accessed, or any consequences resulting from Internet use.

- The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e-Safety complaints and incidents, including any actions taken, will be recorded by the school.

## Use of Internet Outside of School

Although Internet use is carefully controlled within school, most pupils will have access to it outside of school, through a variety of means. The school recognises that we have no control over this access, but we hope that the guidelines introduced at school will help them to use it in a safe and responsible manner.

The school will be sensitive to issues related to the use of the Internet outside school, and will discuss any items of concern with parents (for example, access of sites inappropriate to age).

The school's anti-bullying policy covers pupils' behaviour in all settings, in and out of school, and this includes on the Internet. Should any incidences of cyberbullying occur, it will be dealt with as described in that policy.

The school recommends that parents monitor children's Internet use carefully; it is too easy for them to inadvertently access unsuitable sites if they have unrestricted access.

The School e-Safety Coordinator is Mr G Wharton

Policy approved by Head Teacher: Mr G Wharton Date: 27<sup>th</sup> November 2014

Policy approved by Governing Body: Emma Norling

The policy will be reviewed annually.

## APPENDIX 1

### **Bradwell C E (C) Infant School ICT Acceptable Use Policy Pupil Agreement / eSafety Rules**

Bradwell C E (C) Infant School has computers & I-pads with internet access to help our learning. We have a monitoring solution where web based activity is monitored and recorded. The Schools internet access is controlled through EMBC web filtering service.

These rules will keep everyone safe, and help us to be fair to others.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use the Internet and/or online tools when a trusted adult is present.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will only e-mail people I know, or my teacher has approved.
- ✓ The messages I send will be polite and sensible.
- ✓ I will not access other people's files.
- ✓ I will not bring CD ROMS/Memory Sticks from outside school unless I have been given permission
- ✓ I will ask permission from a member of staff before using the internet.
- ✓ If I accidentally find anything inappropriate I will tell my teacher immediately.
- ✓ I will report any unpleasant material or message sent to me. I understand my report will be confidential and will help protect other pupils and myself.
- ✓ I will not give out my own, or others' details such as names, phone numbers or home addresses.
- ✓ I will not attempt to download or install anything on to the school network without permission.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- ✓ I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy & Anti-Bullying Policy (these may be viewed on the School website).