

DRAYTON COMMUNITY INFANT SCHOOL



E safety policy

To underpin the values and ethos of our school and our intent to ensure our children/young people are appropriately safeguarded this policy is included under the safeguarding umbrella.

Approved by governors Spring 2010

Reviewed Spring 2011

E-Safety Policy

What is E-Safety?

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The safe and effective use of the Internet is an essential life-skill, required by all. However, unmediated Internet access brings with it the possibility of placing users in embarrassing, inappropriate and even dangerous situations. The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Children and young people must also learn that publishing personal information could compromise their security and that of others. Services need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children.

The use of NCC equipment for inappropriate reasons is "unauthorised". We will use the measures in place, as described below, to demonstrate safe use.

Routes to E-Safety

The school has appointed an e-safety coordinator/monitor (Mrs Gray and Mrs Besenzi).

Our e-Safety Policy has been written by the school, building on the government guidance. It has been agreed by senior management and approved by governors.

Guided use

Internet use raises educational standards, promotes achievement, supports professional work and enhances management information and business administration systems. Therefore, we will provide safe and secure Internet access (through ICT Solutions). This will be appropriate to

the audience in terms of safeguards and guidance of use. Child users need to be taught that it is only safe to use the internet with adult supervision. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Risk assessment

21st century life presents dangers including violence, racism and exploitation from which people need to be protected. They will need to learn to recognise and avoid these risks - to become "Internet-wise". Risk assessments will be performed to ensure that everyone is fully aware of and can mitigate risks of Internet use. Users will be taught how to cope and what to do if they come across inappropriate material. Users may access the Internet in Libraries, public access points, Youth Clubs and in homes. Ideally a similar approach to risk assessment and E-Safety would be taken in each of these locations. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Responsibility

E-Safety depends on all users taking responsibility. The balance between educating users to take a responsible approach and the use of regulation must be judged carefully. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.

Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access must simply be denied, for instance un-moderated chat rooms present immediate dangers and are banned. Guidelines, clarified by discussion and prominently displayed at the point of access, will help users make responsible decisions. The school (through ICT Solutions) will keep an up-to-date record of access levels granted to all network users. We will take responsibility for regularly checking that filtering and monitoring is appropriate, effective and reasonable, and that technical staff have not taken on themselves the responsibility for educational or disciplinary issues.

Appropriate strategies

The E-Safety policy should describe strategies to help ensure responsible and safe use. They should be based on limiting access, developing responsibility and on guiding users. There are no straightforward or totally effective solutions and users themselves must remain vigilant. We will take all reasonable precautions to ensure that users access only appropriate material.

Filtering will be matched to the user requirements. However, due to the international scale and connected nature of Internet content, it is impossible to guarantee that unsuitable material will never appear on a device, but using the information provided in the e-safety policy guidance will minimise this risk and assist in dealing with situations which may arise.

Published content and the school web site

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. The Head teacher and Deputy Head teacher will take

overall editorial responsibility and ensure that content is accurate and appropriate. Consent will be obtained before images or work is presented on the school website. Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. We will try to use group photographs rather than full-face photos of individual children. Pupils' full names will not be used anywhere on the school Web site or VLE, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. Work can only be published with the permission of the pupil and parents/carers.

Managing filtering

- The school will work with the NCC and ICT Solutions to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

School PC and laptop usage

- All staff who accept responsibility for a school laptop must do so in a professional manner. They must use the laptop for professional school work only and not for personal purposes.

Photography

- Images must only be used after gaining permission from parents/carers.
- All school photography (video and stills) will be done using a school camera. Staff must only upload these images to a school computer (PC/laptop). Whilst on school visits and outings, CRB checked adults will be allowed to take photographs and must adhere to the restrictions as deemed in this policy.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Introducing the e-safety policy to pupils

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training (particularly through the introduction of the VLE to children and parents/carers) in e-Safety will be developed, based on the materials from CEOP.
- e-Safety training will be embedded within the ICT scheme of work.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.
- Staff who use social networking sites, such as Beebo and Facebook, should not accept parents or pupils as 'friends'. They should conduct themselves in a professional manner.
- In order to safeguard all stakeholders, the use of mobile phones is prohibited to rooms where children are not present. Mobile phones **Will not** be used for filming or photography.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the VLE and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

All staff, parents and children will be made aware of school safeguarding procedures as appropriate to their needs.