

**Interview Record**

**Dromore Central Primary School**

**E-Safety Policy**

**Acceptable Use of the Internet Policy**

**June 2023**

**Table of Contents**

1. Introduction Page 3
2. Code of Safe Practice Page 3
3. Mobile Phones Page 4
4. Sanctions Page 4
5. Code of Practice for Staff Page 4
6. Internet Safety Awareness Page 5
7. Inappropriate Content Page 5
8. Excessive Commercialism Page 6
9. Internet Safety Awareness for Pupils Page 6
10. Internet Safety Awareness for Staff Page 6
11. Points for Teachers to Consider Page 6
12. Internet Safety Awareness for Parents Page 7
13. Points for Parents to Consider Page 7
14. Health and Safety Page 7
15. Digital and Video Images of Pupils Page 8
16. School Website Page 8
17. Storage of Images Page 8
18. Social Software Page 8
19. Policy Review Page 9

Acceptable Use of the Internet & Digital Technology Policy

Ratified by Board of Governors (Date)\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Review Date: June 2023

**Introduction**

In Dromore Central Primary School, we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform learning and teaching when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. Our school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them in a safe, responsible manner.

“Used well, digital technologies are powerful, worthwhile educational tools. Technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools.”

This document sets out the policy and practices for safe and effective use of the internet in Dromore Central Primary School. This policy has been drawn up by the ICT Coordinators under the leadership of the Principal, with valuable input from the staff. It has been approved by Governors and is made available to all parents through the school website. The policy and its implementation will be reviewed annually.

**Code of Safe Practice**

When using the internet, e-mail systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity.

The Code of Safe Practice for Dromore Central Primary School makes explicit to all users (staff and pupils) what is safe and acceptable and what is not. The scope of the Code covers fixed and mobile Internet; school PCs, iPads, laptops and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, iPads, wearable digital technology etc.) is subject to the same requirements as technology provided by the school. The ICT Co-ordinators will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology. Code of Practice for Pupils Pupil access to the Internet is through a filtered service provided by c2K, which should ensure educational use of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents on child’s enrolment before pupils access the Internet. Both parties sign this ICT Code of Practice. Agreement and copies of these are held in Confidential Pupil Folders. A class over-view sheet should also be completed by the class teacher for quick reference with a copy sent to co-ordinators for filing.

In addition, the following key measures have been adopted by DCPS to ensure our pupils do not access any inappropriate material:

* The school’s E-Safety SMART targets for use of the Internet and other digital technologies is made explicit to all pupils and is displayed prominently in our computer areas and classrooms;
* Our Code of Practice is reviewed each school year;
* Pupils using the Internet will normally be working in highly-visible areas of the school;
* All online activity is for appropriate educational purposes and is supervised, where possible. Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group;
* Pupils in Key Stage 2 are educated in the safe and effective use of the Internet, through a number of selected programmes and assemblies. It should be accepted, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor c2K can accept liability under such circumstances.

**Mobile Phones / Wearable Digital Teachnology**

The use of mobile phones by pupils is not normally permitted on the school premises during school hours, unless in exceptional circumstances, where the Principal/ Vice Principal/Head of Key Stage will authorise its use. During school hours, pupils are forbidden to remove their phones from their school bags/switch them on, unless specifically assigned by the teacher. Children should not be wearing digital devices to school e.g. watches that have the function to record / phone. If a device is brought to school, the child will be asked by the class teacher to remove it and place it in a secure place until the end of the school day when it will be returned.

**Sanctions**

Incidents of technology misuse which arise will be dealt with in accordance with the school’s discipline policy. Minor incidents will be dealt with by the Principal/ICT Co-ordinator and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with school child protection procedures.

**Code of Practice for Staff**

Staff have agreed to the following Code of Safe Practice:

Pupils accessing the Internet should be supervised by an adult. All pupils are aware of the rules for the safe and effective use of the Internet. These are displayed in prominent locations within the school and discussed with pupils. All pupils using the Internet have written permission from their parents. Recommended websites for each year group are available from Year Group Leaders. Any additional websites used by pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age-appropriate. Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/ICT Co-ordinators. In the interests of system security, staff passwords should *only* be shared with the network manager.

Teachers are aware that the c2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users. Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.

Photographs of pupils should, where possible, be taken with a school iPad/camera and images should be stored on a centralised area on the school network, accessible only to teaching staff. Images can be shared to the school’s social media only with prior agreement from the parents. School systems may not be used for unauthorised commercial transactions.

**Internet Safety Awareness**

In DCPS we believe that, alongside having a written safety policy and code of practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

**What are the Dangers?**

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable.

**Key Concerns are:**

Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use chat rooms or e-mail to communicate with children for inappropriate reasons.

Children need to be taught:

• That people are not always who they say they are.

• That “Stranger Danger” applies to the people they encounter through the Internet.

• That they should never give out personal details or

• That they should never meet alone anyone contacted via the Internet

**Inappropriate Content**

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content. Materials may express extreme views e.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere. Materials may contain misleading and inaccurate information e.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

Children need to be taught:

• That information on the Internet is not always accurate or true.

• To question the source of information.

• How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

**Excessive Commercialism**

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive. Children should be taught:

• Not to fill out forms with a lot of personal details.

• Not to use an adult’s credit card number to order online products. If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

**Internet Safety Awareness for Pupils**

Rules for the Acceptable use of the Internet are discussed with all pupils and are prominently displayed in prominent areas in the school. In addition, Key Stage 2 pupils follow a structured programme of Internet Safety Awareness through Google. This includes lessons taught in class and assemblies attended annually.

**Internet Safety Awareness for Staff**

The ICT Co-ordinators keep informed and updated on issues relating to Internet Safety and attend regular courses. This training is then disseminated to all teaching staff, classroom assistants and supervisory assistants on a regular basis.

**Points for Teachers to Consider**

Internet use should be planned, task orientated and educational within a regulated and managed environment. Supervision is the key strategy. Children should have a teacher or classroom assistant present when using the Internet. Children should know why they are using the Internet. Teach children to use the Internet in response to a need e.g. to answer a question which has arisen from work in class. Search engines require careful use and planning/supervision. Children can be bombarded with information and yet fail to find the material they need. Children do not need thousands of website addresses. A small appropriate choice is much more effective. Individual e-mail addresses may not be considered appropriate for younger children, FS and KS1. Individual or teacher e-mail addresses may be used in KS2 where appropriate and with the permission of the class teacher. All incoming and outgoing mail should be checked. Discuss with pupils the rules for responsible Internet use. It is not enough to protect children from materials, we must teach them to become Internet Wise. Children need to learn to recognise and avoid the risks. Children need to know what to do if they come across inappropriate material or if they are approached by a stranger. Be informed – read about E-Safety.

**Internet Safety Awareness for Parents**

The Internet Safety Policy is available for parents by request and is also posted on the school website. The Code of practice for pupils is sent home at the start of Year 1 for parental signature. Internet safety leaflets for parents and carers are also sent home biannually.

**Points for Parents to Consider**

It is important to promote Internet Safety in the home and to monitor Internet use. Keep the computer in a communal area of the home.

• Ask children how the computer works.

• Monitor on-line time and be aware of excessive hours spent on the Internet.

• Take an interest in what children are doing and the online games they are playing. Discuss with the children what they are seeing and using on the Internet.

• Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.

• Discuss the fact that there are websites which are unsuitable.

• Discuss how children should respond to unsuitable materials or requests.

• Remind children never to give out personal information on the Internet.

• Remind children that people on line may not be who they say they are.

• Be vigilant. Ensure that children do not arrange to meet someone they meet on line.

• Be aware that children may be using the Internet in places other than in their own home or at school.

**Health and Safety**

DCPS have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the resource areas. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used.

**Digital and Video Images of Pupils**

Parental permission is sought at the start of Year 1 to cover the use of photographs of pupils on the school website, in the local press and for displays etc within school and written permission must be obtained from the parent/carer.

**School Website/Facebook**

Our school website and Facebook page promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life. In order to minimise risks of any images of pupils being used inappropriately the following steps are taken:

* Group photos are used where possible, with general labels/captions;
* Surnames are not used
* no home addresses, telephone numbers, personal emails or any other personal information about pupils or staff are included
* Website links selected by teachers will be previewed and checked regularly.
* Parents’/Carers’ permission will be sought to publish pupils work and/or photographs. These will only be published subject to the strict safeguards above.

**Storage of images**

Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area on the school network, accessible only to teaching staff. Photographs of pupils are removed when they leave the school.

**Social Software**

Chat-rooms and other social networking sites are blocked by the c2K filters so pupils do not have access to them in the school environment. However, we regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils. Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school’s discipline policy and child protection procedures. Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

All reasonable and appropriate steps have been taken to protect pupils. The school recognises that despite employing safety procedures, in some circumstances, the Internet may give children access to undesirable information or images. Children are regularly reminded that should they encounter inappropriate material online they must immediately leave that website and inform an adult.

Should a child or teacher encounter unsuitable material through the managed service, this will be reported to c2k via the c2k helpdesk number.

**Policy Review**

Internet technology and school use of resources will develop and change with time. It is our intention to revise and up-date our Internet Safety Policy as appropriate and where necessary.