RICHMOND PRIMARY SCHOOL

E-Safety Policy

Reviewed November 2020

RICHMOND PRIMARY SCHOOL

ACCEPTABLE USE OF THE INTERNET AND DIGITAL TECHNOLOGIES

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools

1. Introduction

In Richmond PS we believe that the Internet and other digital technologies are very powerful resources which can enhance teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This 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.

The above circular states that:

> *"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 the safe and effective use of the Internet in our school. The policy has been drawn up by the staff of the school under the leadership of the Principal/ICT Co-ordinator.

The policy and its implementation will be reviewed annually.

2. Code of Safe Practice

When using the Internet, email 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 Richmond PS 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, laptops, ipods, tablets, ipads, kindles, digital cameras, other electronic devices and digital video equipment. It should also be noted that the use

of mobile devices owned personally by staff but brought onto school premises (such as mobile phones, camera phones, PDAs, Ipads, ipods) is subject to the same requirements as technology provided by the school. Under Child Protection, devices owned personally by pupils should not be brought into school and should not be used to record/store still or moving images in school. Any storage devices containing school data should be password protected.

The ICT Co-ordinator will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

"Teachers and parents both have a role in educating our young people on using the internet appropriately. Teachers can give pupils opportunities to use and create positive online content and at the same time give them the confidence and the skills to seek help should they encounter problems online. Parents can help by showing an interest and having discussions with their children about their online activity" Minister of Education 10th February 2015.
From time to time parents are also invited to school for an information evening by PSNI on Internet Safety.

- **Code of Practice for pupils**
  Pupil access to the Internet is through a filtered service provided by C2K, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents on an annual basis before pupils access the Internet.

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

  o The school's Code of Practice for use of the Internet and other digital technologies is made explicit to all pupils and is displayed prominently; (SMART ICT RULES)
  o Our Code of Practice is reviewed each school year and signed by pupils/parents;
  o Pupils using the Internet will normally be working in highly-visible areas of the school;
  o 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 are educated in the safe and effective use of the Internet, through a number of selected activities including Police visits, PDMU lessons, Child Protection Assemblies and Safer Internet Day.

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither Richmond PS nor C2K can accept liability under such circumstances.

The use of mobile phones by pupils is not permitted on the school premises during school hours, or on school trips or residential trips unless in exceptional circumstances, where permission may be granted by the Principal.

During school hours, pupils are forbidden to play computer games or access social networking sites, unless specifically assigned by the teacher. Pupils should not bring electronic devices to school.

♦ **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 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 agreed to the following Code of Safe Practice:

- Pupils accessing the Internet be should supervised by an adult.
- All pupils are aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils.
- All pupils using the Internet have <u>written permission from their parents.</u>
- <u>Websites used by pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age-appropriate.</u>

- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal and ICT Co-ordinator.
- In the interests of system security staff passwords should not be shared with anyone.
- 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.
- School systems may not be used for unauthorised commercial transactions.

3. Internet Safety Awareness

In Richmond PS 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.

- **Internet Safety Awareness for pupils**

Rules for the Acceptable use of the Internet are discussed with all pupils and are prominently displayed in classrooms. Pupils complete Internet Safety Awareness using a range of online resources and visits from PSNI, during assemblies, PDMU and a special focus on Internet Safety Day

- **Internet Safety Awareness for staff**

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety and attends regular courses. This training is then disseminated to all teaching staff and classroom assistants.

- **Internet Safety Awareness for parents**

The Internet Safety Policy is available on the school website or from the school office by request and a copy of the Code of practice for pupils is sent home at the start of each school year for parental signature. Internet safety leaflets for parents and carers also are sent home annually.

4.   Health and Safety

Richmond PS have attempted to ensure a safe working environment for pupils and teachers using ICT resources which have been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used.

5.   Digital and Video Images of Pupils

Parental permission is sought at the start of each school year to cover the use of photographs of pupils (e.g. on the school website, in the local press, for marketing purposes and for displays etc within school) and written permission must be obtained from parent/carer.

♦ **School Website**
The BOG have agreed that the sole purpose of the school website is to promote the school and provide information for prospective parents. The password should only be made available to the Principal and ICT Co-ordinator.

The following steps have been taken to protect pupils:
- o Group photos are used where possible, with general labels/captions;
- o Full names are not included alongside photos.
- o The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

♦ **Storage of images**
Digital and video images of pupils are, where possible, taken with school equipment.

6.   Social Net-working Sites

It is important to recognise that there are issues regarding the appropriateness of some content and contact in relation to social net-working sites. Staff are therefore encouraged to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. Images once on-line can never be removed.

- Pupil access to social net-working sites using C2K computers is forbidden.

- Staff should not discuss any school related business on social net-working sites.

- Images of pupils or staff are not to be uploaded on to social net-working sites without the permission of the staff member/s involved.

- It is strongly recommended that staff do not engage with parents on social net-working sites.

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 through PDMU lessons, visits from the Community Police Officer and the P6 "Bee Safe" programme as well as Safer Internet Day activities each February.

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.

7.   E-mail

The use of e-mail within school is an essential means of communication for staff.

- The school gives all staff their own e-mail account to use as a work-based tool. By using your own school e-mail account you are clearly identified as the originator of a message.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and

recipients all mail is filtered and logged. If necessary e-mail histories can be traced.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal (non c2k) e-mail addresses.
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- Staff must inform the Principal if they receive an offensive e-mail.
- However you access your c2k e-mail (whether directly, through web mail when away from school or on non-school hardware) all the school e-mail policies apply.

8. Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use during non-contact time with pupils.
- The school discourages members of staff contacting a parent/carer using their personal device.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, laptops and PDA for off-site visits and trips, only these devices should be used.

If a parent has a concern about any aspect of this policy, he or she is invited to contact the ICT Co-ordinator Mrs Haslett, or the school Principal Mrs Robinson.

This policy will be reviewed annually in light of technological advances.

Signed :- _____ Chair of B.O.G

Date

Richmond Primary School

ICT Code of Practice Agreement for Pupils and Parents

The school has installed computers, ipads and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will access the system with my login and password, which I will keep secret.

- I will not access other people's files without permission.

- **I will only use the computers for school work and homework.**

- **I will not bring software or CDs into school without permission.**

- **I will not bring any personal mobile device without the Principal's permission**

- **I will ask permission from a member of staff before using the Internet.**

- **I will not disclose my home address or telephone number, or arrange to meet anyone.**

- **I will report any unpleasant material or messages sent to me.**

- **I understand that the school may check my computer files and may monitor the Internet sites I visit.**

- **I will not use Social Media sites on any school machine and I will only use websites approved by my teacher.**

- **I will not take photographs from the school website and upload on any social media site**

- **I will never give out personal information or passwords.**

Signed by child: _____

Signed by parent/guardian: _____

Date: _____

A   ors)

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff and Governors are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- I will only use the school's e-mail/internet/and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or C2k.
- I will ensure that all electronic communications with staff are compatible with my professional role.
- I will not give out my own personal details such as mobile phone number and personal e-mail address to pupils.

- I have been advised not to give out my own personal details such as mobile phone number and personal e-mail address to parents/carers.
- I will ensure that school personal data is kept secure and is used appropriately, whether in school taken off the school premises or accessed remotely. All personal or sensitive data taken off-site must be encrypted on a teacher laptop (provided by C2k or on an encrypted external drive provided by the school.
- I will not install any hardware or software without the permission of the ICT co-ordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken stored and used for professional purposes in line with school policy and with written consent of the parent/carer or staff member.
- I will support the school approach to on-line safety and not deliberately share or upload any images, video or text that could upset or offend any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request to the Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my on-line activity, both in school and outside school will not bring Richmond PS or my professional role into disrepute.
- I will support and promote the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies in the context of school.
- I understand the sanctions related to breaches of the above.

<u>User Signature</u>

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Full Name (Printed)   _____

Signature   _____

Date   _____