St Columba's P.S.
Newbuildings

E Safety Policy

Reviewed by staff: June 2016

Ratified by BOG: October 2017

Review Date: Prior to June 2019

Introduction

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety. The policy relates to other policies including ICT curriculum, Internet Access, Bullying, Child Protection and Health and Safety.

Teaching and Learning

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.
Access to the Internet is a necessary tool for staff and students and is a requirement within the NI Curriculum.
It helps to prepare students for their on-going career and personal development needs.

Internet Use To Enhance Learning

Internet access within St Columba's is provided by c2kni and is designed for to be safe for all users. This includes each individual having their own log-in and password, as well as filtering content appropriate to the age of pupils. Access to the internet is planned to enrich and extend learning and is reviewed to reflect the appropriate curriculum requirements.
When age-appropriate, pupils are

- Given clear guidance on safe use of the Internet, are taught how to take responsibility for their own Internet access and sign an Internet Use agreement
- Are taught ways to validate information before accepting that it is necessarily accurate
- Are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed
- Are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Managing Internet Access

System Security

Our school computer network is managed by c2kni to ensure that it is safe and appropriate for pupils.

E-mail (Pupils)

As yet, pupils do not have access to school-based e-mail accounts but they are made aware that

- They must be very vigilant about using e-mail as a means of communication
- Must tell a teacher immediately if they receive offensive email
- They must not reveal their personal details, those of others or arrange to meet anyone without specific permission from their parents
- They should not open suspicious incoming email or attachments.

E-mail (Staff)
C2k recommend that all staff should be encouraged to use their C2k email system. It is strongly advised that staff should not use home email accounts for school business.
The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

Social Networking (Facebook etc)
Pupils will not have access to sites such as Facebook etc. inside school, but we are very aware that social networking has become a huge part of many children's online activity. Indeed, we realise that many of our pupils will have Facebook, Snapchat, Instagram, TIk-Tok, accounts at home, and we therefore aim to build their awareness as to how to use these sites appropriately. As part of our ICT programme, pupils will be informed

- To keep personal safety to the fore when using such sites
- Not to get involved in any form of online/cyber-bullying
- That parents will be informed immediately of any breaches either during or after school

Occasionally, pupils will use chat rooms within the c2kni network e.g. Fronter as part of supervised class ICT activity but only when using the filtered network within school and only when supervised by an adult.

Cyber Bullying
Staff are aware that pupils may, from time to time, be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is considered within the school's overall anti-bullying policy and pastoral services as well as the e-Safety policy.

- Cyber Bullying can take many different forms and guises including:
- Email – nasty or abusive emails which may include viruses or inappropriate content
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites
- Mobile Phones – examples can include abusive texts, video or photo messages.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that all incidents of cyber-bullying will be treated within the school's Anti-Bullying Policy

Use of Images on School Web Site/Facebook Page
Our school online presence complies with the school's guidelines for using images. For example,

- Photographs used will not identify individual pupils.
- Children's photographs are only used once prior written permission has been received from the child's parents
- Children's photographs are not accompanied by names.
- Children's work which contains photographs must not also contain the child's name.

Filtering of Content
The school works in partnership with parents, DENI, EA and c2kni to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover unsuitable sites, they are informed that the URL (address) and content must be reported to the ICT co-ordinator who will then inform c2k.

Managing Video Conferencing
Video conferencing is used in upper Key Stage 2 classes and uses only the approved program. Pupils are made aware of the need to behave appropriately and are always supervised by an adult.
Access to video conferencing is always appropriately planned and managed by members of staff. Pupils have no independent access to webcams etc.

Managing Mobile Phone Technologies

- Children are not permitted to bring phones to school and if it is deemed necessary by parents e.g. child going home alone on bus. They must be handed to the teacher at the beginning of the day switched off and it will be returned to them at the end of the school day.
- Mobile phones must not be used during teaching time for calls or text messages. If staff need to be contacted urgently during the school day this can be done via the school office
- Cameras in mobile phones are not used by staff or pupils
- Smartphones are not to be used within the school day to access the internet
- Only school cameras are used by both staff and children for educational purposes.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.

Policy Decisions

Authorising Internet access

All staff must read and sign the “Staff Code of Conduct for ICT” before using any school ICT source.
The school maintains a record of all staff and children who have access to the school’s ICT systems.
Parents are asked to sign a consent form regarding their child’s internet use (see Acceptable Use Policy).
Any person not directly employed by the school will be asked to read and sign the “Acceptable Use of School ICT Resources” before being allowed to access the internet from the school site.

Assessing risks

The school takes 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. The school will endeavour to ensure that inappropriate content is not accessed but cannot accept liability if any such material evades our filtering systems. The school’s e-safety policy and its implementation will be monitored and reviewed on a regular basis.

As part of their learning, children will be made aware, as appropriate, of the needs to protect themselves from harmful material whist online. This will be done on an age-appropriate basis.

Pupils will know that they are to inform an adult if any inappropriate material becomes evident during the school day.

Handling E-safety Complaints

- Complaints of pupil/staff internet misuse must be referred to the principal, Mrs Callan
- Complaints of a child protection nature will be dealt with in accordance with the school’s Child Protection policy.
- Pupils and parents are informed of the complaints procedure.
- Pupils and parents are informed of the consequences for pupil misuse of the Internet (see Acceptable Use Policy).

Communications Policy

Introducing the e-safety policy to pupils

E-safety posters are posted next to all computers so that all users can see them.

Pupils are informed that network and Internet use is monitored and appropriately followed up.

The children receive e-safety lessons and are constantly reminded of online safety.

Staff and the E-safety policy

All staff are trained to monitor children’s Internet use and receive a copy of the e-safety policy. Staff are informed that network and Internet traffic can be traced to an individual user.

Enlisting Parents'/Carers' Support

Parents’ and carers’ attention is drawn to the school’s E-safety Policy in newsletters, the school brochure and on the school website.

The school has links on its Facebook page to e-safety resources and resources to help support parents e.g. common sense media.
The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.

Appendix 1

St Columba's Primary School
CODE OF PRACTICE FOR THE RESPONSIBLE USE OF COMPUTERS AND DIGITAL TECHNOLOGIES

St Columba's Primary School has a networked computer system, which is filtered and controlled by C2Kni. This filtered system enables staff and children to share and store materials electronically and to access a limited number of Internet sites which are of educational value.
Children in St Columba's PS will only access the filtered Internet connection under strict supervision by their teacher and will therefore not have any opportunities to freely "surf the net". Using ICT is an essential tool, which is used to promote and enhance all aspects of teaching and learning throughout the curriculum. It is therefore important that all children in our school have the opportunities to benefit from the experiences gained by using these readily available resources.
There are now opportunities in school for children to use electronic gadgets such as iPads, BeeBots and Roamers, and to use digital cameras to acquire still pictures and video for presentation and display purposes. Again, it is essential that these are used under strict guidelines and supervision.

The following 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 in software or pen-drives/CDs into school without permission.

I will never use my mobile phone in school to take photographs or to video my friends or others.

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

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

I will immediately report any unpleasant material or messages sent to me. If it happens at home, I will immediately talk to my parents/carers.

Children in Key Stage 2 classes will occasionally have opportunities to communicate with each other via email or video conferencing. These rules will again keep everyone safe and promote learning in a positive and creative way for all involved.

I will only use video-conferencing when this is arranged by my teacher

I will not use Internet chat-rooms in school.

I will always use language that is supportive and kind when online.

I will never give out personal information or passwords.

Any messages I send will be polite and responsible.

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

Appendix 2
School-Based Internet Access

Dear Parent/Carer

As part of St Columba's PS' Information and Communications Technology (ICT) programme, we offer pupils supervised access to a secure and filtered Internet service that is provided across all N. Ireland schools by an organisation called C2K. Access to the Internet allows pupils to explore and make appropriate use of many web sites that are of enormous benefit, but as we all know too well, there are many dangers online as well.

In order to minimise any risks which might arise from school-based Internet use, C2K has installed very effective filtering software which successfully blocks thousands of potentially inappropriate or offensive sites. It also bars any internet access via the use of inappropriate terms/words by pupils in search engines. To further enhance security, pupils only use the internet for educational purposes, under the supervision of a member of staff.

The school's rules for safe Internet use accompany this letter. Please read it carefully, discuss it with your child and then return the slip below. If you have any concerns or would like further clarification of school-based internet access, please contact me here in school at any time.

Yours sincerely,

Mrs Caroline Callan
Principal

School-Based Internet Access

I have discussed the school's internet rules with my child, who agrees to follow the eSafety rules and to support the safe use of ICT at home and at St Columba's.

Child's Name: _____ Class: _____

Parent/Carer Signature: _____