WHITEABBEY

PRIMARY SCHOOL

Safe and Effective Use Policy for the Internet and Digital Technologies in School

Revised September 2017

Dear Parent,

The Board of Governors in Whiteabbey Primary School has a policy on the safe, healthy, acceptable and effective use of the Internet and other digital tools, (e.g.: digital cameras, acceptable use of mobile telephones & hand-held gaming devices which have downloadable capabilities). They also promote safe and acceptable practices for all staff and pupils.

Please read these guidelines for the use of the Internet in Whiteabbey Primary School. The Department of Education has stated that each school must have these policies in place regarding safeguards, accessibility and supervision.

Whiteabbey staff will ensure that with your help the rules and guidelines stated in this booklet are reinforced to the best of our ability. Please read them carefully with your child. Parts of this booklet are based on "Acceptable Use of the Internet and Digital Technologies in Schools", (DENI Circular 2007/1 – 18 June 2007), "Internet Safety" (DENI 2011/22 – 27 September 2011) and "eSafety Guidance" (DENI 2013/25 – 6 December 2013).

In accordance with the Department of Education it is necessary for you to give permission for your son/daughter to use the Internet in school. We would appreciate your help in expediting this by completing the "ICT Parental Permission Agreement" sheet sent out at the beginning of each school year and returning it to your child's class teacher.

Any parent who wishes to discuss this policy can contact the school and put any questions to:
Mr K. Wysner (Principal)
Mrs N. Gray (ICT Co-ordinator)

All users should read and familiarise themselves with the terms of this policy. Indeed it is an explicit condition of the use of Information and Communications Technology, (ICT), in Whiteabbey Primary School that pupils and parents agree to the terms contained.

Contents.

1. Introduction.

Rationale

At Whiteabbey, we encourage use by pupils of the rich information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. Staff and pupils are encouraged to use this resource well and safely. Wherever possible, staff will select online resources designed specifically for pupil use. At times, the Internet may provide access to information that has not been selected by the member of staff. At Whiteabbey the Internet is filtered by C2k and Classnet who at all times will try to ensure that pupils do not access any inappropriate and unwanted information.

Key Principles

This policy rests on four key principles:

i) **Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop ICT life skills in their use.**
The Internet and other technology-based tools are very powerful resources that can enhance and potentially transform teaching and learning when used effectively and appropriately.

ii) **Technical safeguards are provided and maintained by C2K and Classnet to ensure that the educational use made of such tools within schools is safe and secure, while protecting both the users and the systems from abuse.**
It must be accepted, however, that no matter how rigorous such measures may be, they will never be completely effective.

iii) Ensuring that all users are taught, and that they learn and exhibit, safe, responsible, ethical, moral, legal, healthy, intelligent and effective working practices.
This is an important educational goal which is our responsibility as a school to promote, and for staff to model, at all times.

iv) Deliberate abuses which arise within school should be subject to the rules and regulations of the school; and as a school we will ensure that our rules and regulations are kept up to date to enable the pupils to act appropriately and effectively when required (see Rules Appendix 1)
Deliberate abuses which happen outside school, whether present or past pupils, but which impinge upon or affect school pupils and staff, will be dealt with through appropriate police and legal action.

2. Management Responsibilities.

- Network administrators

C2k reserve the right to review files and communications to maintain system integrity and ensure that the users are using the system responsibly. They will respect the right to privacy whenever possible.

- Staff

This policy has been devised following guidelines from Department of Education, (Circular 2007/01 & 2013/25), and is endorsed by both the Principal and Governors as it is implemented throughout the school. As ICT Coordinator Mrs Gray is responsible for all Internet Safety issues within the school and, in conjunction with the School Management Team, will review this policy.

- Pupils

Key Stage Two pupils, (P4 – P7), have unique usernames and passwords. Pupils must be aware that the ICT Co-ordinator, Principal and staff reserve the right to enter any pupil's folder. Pupils must remember correct netiquette when communicating online and be aware that any e-mails sent from within school are traceable by network administers, Principal, ICT co-ordinator and class teachers. Pupils must not connect to the Internet for unapproved purposes.

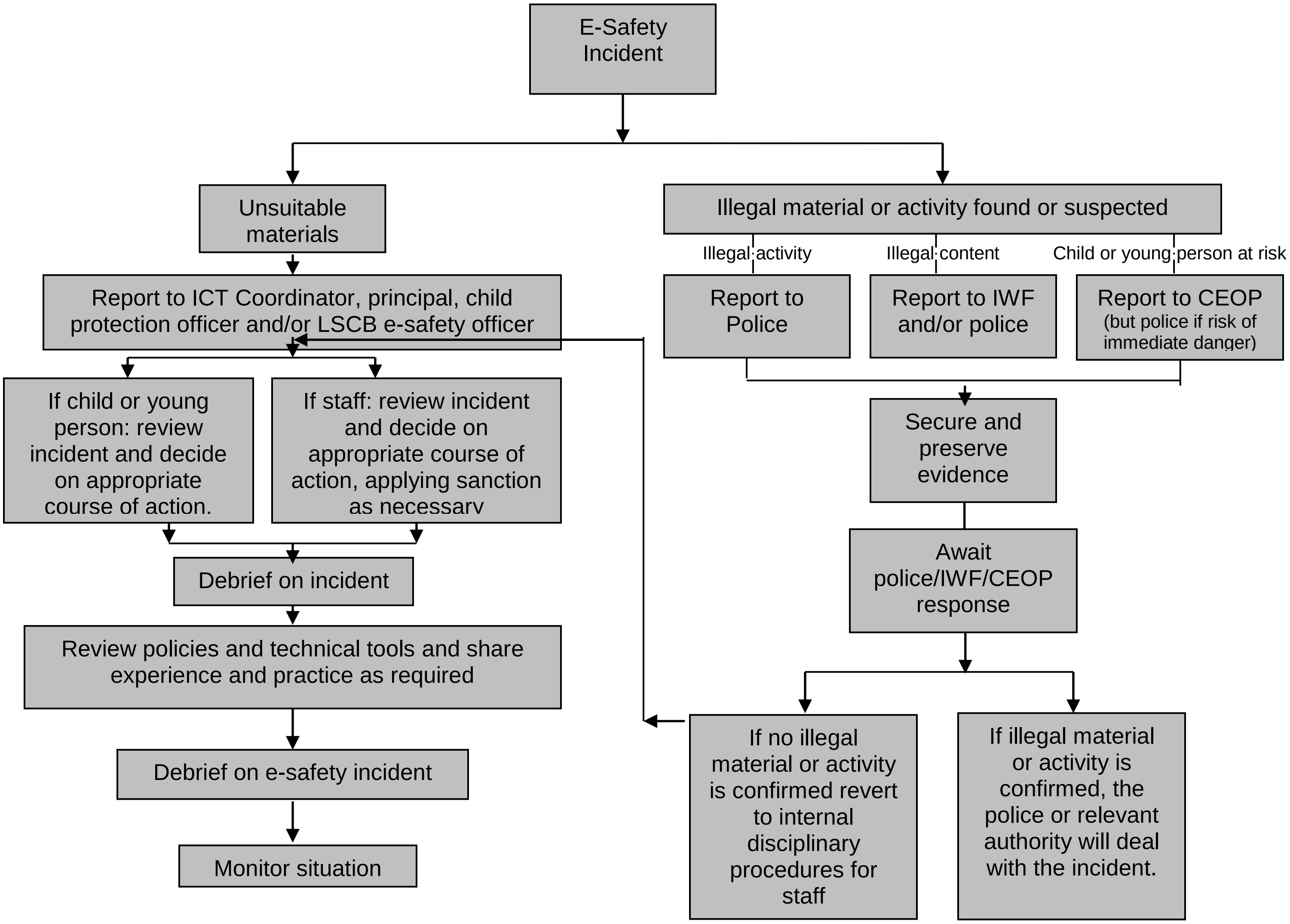
- Parents

Parents must be aware that the access to the Internet provided to staff and pupils in school has limiting security features but that it is closely monitored by staff. The use of ICT is complimentary to the teaching already taking place and should be viewed as a valuable tool to enhance learning.

Parents should, in co-operation with staff, make children aware of the rules and expectations within this Policy and support the prohibition of mobile telephones within school on the grounds that Internet access then becomes difficult to police.
Parents should also be aware that social networking sites such as Facebook adhere to a strict 'over 13's' age policy.

- Managing and reporting incidents and securing evidence of misuse.

The school has procedures in place to deal with any incidents of technology misuse which arise. Minor incidents, (such as plagiarism or copyright infringement, downloading materials not relevant to a subject, using someone else's password, nuisance e-mails), will be dealt with by the class teacher. Parents will be informed if a more serious incident occurs and disciplinary procedures will be implemented. The following flow-chart highlights the schools policy for responding to Internet Safety incidents.


E-Safety Incident
Unsuitable materials
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child or young person at risk
Report to ICT Coordinator, principal, child protection officer and/or LSCB e-safety officer
Report to Police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
If child or young person: review incident and decide on appropriate course of action.
If staff: review incident and decide on appropriate course of action, applying sanction as necessary
Secure and preserve evidence
Debrief on incident
Await police/IWF/CEOP response
Review policies and technical tools and share experience and practice as required
If no illegal material or activity is confirmed revert to internal disciplinary procedures for staff
If illegal material or activity is confirmed, the police or relevant authority will deal with the incident.
Debrief on e-safety incident
Monitor situation

Source: BECTA

3. Code of Safe Practice for Safe and Effective Use.

❖ School Code of Practice

As a school we expect all users, (staff and pupils), to use internet, E-mail and digital technologies in a safe and acceptable manner. All users must be aware that the use of the Internet in schools is a privilege and not a right and this privilege will be withdrawn if it is misused. Both staff and pupils must limit their use of the Internet for school related purposes – examples of this include the use of e-mail, the use of the Internet to investigate and research school subjects and staff using the Internet to further develop their professional development.

Guidelines include:

✓ using all ICT equipment with care and respect;
✓ using ICT in support of the aims and objectives of the NI Curriculum;

- ✓ behaving in an appropriate manner when communicating online;
- ✓ not using obscene or racist language;
- ✓ refraining from sending offensive messages;
- ✓ respecting other user's private folders, documents and files;
- ✓ adhering to copyright laws;
- ✓ following the ICT Suite Code of Practice;
- ✓ agreeing to C2K on line learning environment terms and conditions
- ✓ using resources wisely (including on-line time and printers).

This code relates to technologies provided by the school (e.g. laptops, ipads, digital cameras) as well as those owned by staff, but brought onto the premises, (mobile phones, tablets.)

- ❖ Legal monitoring of e-mail and Internet use.

While normal privacy is respected and protected by password controls, as a publicly-funded network, documents and e-mails may be viewed and monitored by network administrators. Staff and pupils should be aware that all searches and websites visited on the Internet, as well as all e-mails sent and received are tracked and recorded. If a user is aware of any inappropriate use of technology a report should be made to their class teacher or ICT Coordinator.

- ❖ Community use of school ICT resources.

In circumstances where the school is used as a community resource, this policy must be adhered to.

4. Education in Safe and Effective Practices.

By promoting Internet safety and educating themselves, all adults reinforce the messages taught in school and help to equip the pupils with the skills needed to use technology safely, especially where the filtering and firewalls on C2K systems are not available.

i. Professional Development for Teachers

Teachers are the first line of defence in eSafety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to illegal activity. Staff avail of training and support to determine what action is appropriate including when to report an incident of concern to the school Designated Teacher for Child Protection, the Principal or ICT co-ordinator. Additional support and advice can be sought from C2k, Social Services or the PSNI if required.

ii Education of Pupils

The Internet is an integral part of pupils' lives, both inside and outside school. There are ways for pupils to experience the benefits of communicating online with their peers, in relative safety. Many resources are available as useful teaching tools for all Key Stages looking at Internet safety and are usefully incorporated into the ICT programme.

Further information is available from the following websites:
www.thinkuknow.co.uk
www.ceop.police.uk
www.childnet.com

http://www.nspcc.org.uk/shareaware
https://www.**ceop**.police.uk
http://www.parentscentre.gov.uk/usingcomputersandtheinternet/
http://www.kidsmart.org.uk/parents

5. e-Learning.

❖ ‘My School’

The school has a managed computer service supported by C2K which provides us with computers in our computer suite, every classroom and a number of high quality laptops. We have Interactive Whiteboards in every classroom a wireless network that allows children to access their individual documents, the internet and a local printer to support their e-Learning skills development.
‘My School’ is an online tool that has some of the following features:

a. Communication tools, (e-mail, bulletin boards);
b. Collaboration tools, (online forums, intranets, electronic diaries and calendars);
c. Tools to create online content and courses;
d. Online assessment and marking;
e. Controlled access to curriculum resources; e.g.: Newsdesk, online educational videos and an area to store files.

6. Health and Safety Policy.

❖ General guidance.

An adult should always supervise children when they are accessing information via the Internet. Our service providers, C2K and Classnet, filter information, any breaches of this should be reported at once to the helpline: 0870 6011666. It is the responsibility of teachers to ensure their class leaves the ICT Suite clean and tidy after use. Food and drink should not be consumed near ICT equipment.

❖ Safe location and supervision of computers in school.

All computers are located in highly visible areas of the school. In the majority of cases all computer access is supervised, however on occasions, Key Stage 2 pupils may be given permission to use systems independent of staff supervision. In these cases pupils should be implementing the code of practice.

- <u>Posture – ergonomics.</u>

The length of time they will be seated during an ICT session will be no longer than an hour. Children will be made aware of the dangers of prolonged use of computers and incorrect posture

- <u>Interactive Whiteaboards and projectors.</u>

As well as instructing the children in the correct use of Interactive Whiteboards, pupils will be instructed of the dangers of looking directly into the beam of the projector.

7. <u>Photographs, Digital Publishing and Software Licensing.</u>

- <u>Digital and video images of pupils.</u>

In keeping with good practice relating to child protection, parental permission is sought for the use of children's photographs in connection with school.
In the past children's photographs have been used in a number of ways:

a. Photographs of children are regularly taken in school of teams, choir, classes or other groups, individual awards or performances, school trips, school events, etc. Many of these are displayed throughout the school in classrooms and corridors.
b. Photographs of groups and individual children may be put on the school website. Only first names of children will be used. In the unlikely event of any part of the website content causing concern please inform the principal.
c. The school is sometimes promoted through local publications.
d. Photographs are taken of children on special occasions and sent to the local newspaper for publication.
e. Stored and used when forming part of the school's history, such as anniversary celebrations.

- <u>Making and storing digital and video images.</u>

Digital images of pupils captured within school and on trips are stored within the school server which is managed securely by C2K. While the majority are deleted when no longer required, some are stored forming part of the schools history.

- <u>Copyright, Intellectual Property Rights and Creative Commons Licenses.</u>

As a school we actively discourage any kind of plagiarism and teach pupils how to conduct internet research in an acceptable way. This is also applicable to homework.
If staff or pupils are required to use a photograph, song, web page or an article they must observe restriction rights.

8. <u>E-mail and Netiquette.</u>

E-mail is an important form of communication within school. 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.

The term “netiquette” comes from the words “network” and “etiquette”. It refers to maintaining good manners when interacting with others while online. At Whiteabbey we foster good standards of Internet behaviour and provide guidelines for pupils to follow when communicating in an e-mail:

a. Keep personal details, name, telephone number and address a secret.
b. Never send a photograph of yourself or your friends to anyone.
c. Always tell your teacher if you receive something that upsets you.
d. Do not send an e-mail that someone else wrote without their permission
e. Always give your message a subject. This will give readers an idea of what is in the message. Keep your message short and simple.
f. Remember all e-mails sent from school are traceable by adults.

9. Social Software.

Social software is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks and Blogs (personal web journals.) C2K filters out these social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment. For this reason concern about inappropriate activities would tend to come from use outside the school environment.

The minimum age for sites such as Instagram and Facebook is 13. Whiteabbey Primary School do not promote the use of these sites or any repercussions that may result from comments posted. “A Parent’s Guide to Facebook” is available online www.connectsafely.org/safety-advice-articles/facebook-for-parents.html

- Perceived age restrictions on these sites are fairly meaningless and easily circumvented with both adult and child content then available to view.
- When using these outside school, users should be careful about the information they disclose and how they interact with unknown contacts.
- Personal Profiles: When publishing personal profiles on these social areas, users should clearly understand the difference between **public** which everyone can see and more closed sites where the user selects who they want to see their profile.
- For this reason it is recommended that users should not disclose significant personal information (especially home or e-mail addresses), either in on-line profiles/weblogs or in communications to unknown contacts.
- Disclosure of personal details leaves users vulnerable and could inadvertently solicit unwelcome interest.
- In some cases users can be targeted or groomed by ill- intentioned individuals (see Child Protection/Child Exploitation and Online Protection – CEOP)
- The same rules apply when using webcams.

- As these popular sites become an ever-increasing part of our daily lives, the education of staff, pupils and parents on the safe and responsible use of social software is paramount.

10. Mobile telephones and hand held gaming devices.

Unless in exceptional circumstances or with prior consent received from the Principal, mobile telephones and hand-held gaming devices with downloadable capabilities are prohibited in school on the grounds that they:

a. Are valuable and may be lost, damaged or stolen;
b. Are capable of storing images that are inappropriate;
c. Are capable of connecting to the Internet and accessing websites that are otherwise filtered out by C2K.

11. Management Information Systems.

❖ Data Protection and school information systems.

Personal data is defined as any combination of data items which identifies an individual and provides specific information about them, their families and their circumstances. Data stored within school is stored following the good practice principles as outlined in the Data Protection Act 1998.

❖ Unauthorised computer use in schools.

Unauthorised access of computer materials, use of the school system for commercial purposes and access of premium rate numbers are all prohibited through the system.

- School systems may not be used for unauthorised commercial transactions.
- Neither teachers nor pupils should use the ICT facilities for private financial gain or for commercial purposes.
- Systems must not be used to offer, provide, or purchase products or services unless prior approval to do so has been given**.**

12. Child Protection.

❖ Cyber Bullying.

Cyber bullying can occur on-line and through mobile phones. School staff, parents and pupils must work together to prevent such behaviour and to tackle it when it occurs.

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. **PLEASE NOTE**:

Social networking sites such as Facebook adhere to a strict 'over 13's' age policy.

- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or inappropriate photo or video 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.

It is important that pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases. Records of cyber-bullying incidents will be kept to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

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 cyber-bullying can constitute a criminal offence.

Useful Websites:
Protection from Harassment (NI) Order 1997
http://www.legislation.gov.uk/nisi/1997/1180
Malicious Communications (NI) Order 1988
http://www.legislation.gov.uk/nisi/1988/1849
The Communications Act 2003
http://www.legislation.gov.uk/ukpga/2003/21

❖ Risk Assessments

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks — to become "Internet-wise" and ultimately good "digital citizens". Pupils are made aware of how to cope if they come across inappropriate material or situations online.

13. Internet Wifi Filtering.

❖ Non C2K internet

The school through detailed testing identified that it required a dedicated internet service to support its mobile device strategy. This system exists in parallel to all C2K infrastructure. In line with DENI Circular provision the school has ensured that this additional service is:
a) Filtered to standardised child protection levels
b) Supported by trained staff in its use
c) Reported to and approved by its Board of Governors.

APPENDIX 1
Whiteabbey Primary School
ICT Rules and Regulations.

e-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access should be made via the user's authorised account and password.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the class teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Foundation & Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can ***search*** the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails as a class with our teacher.

We can write polite and friendly emails to other pupils in the school.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- I log on to the computer as myself.
- I will ask permission from my teacher before using the Internet.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- I will only e-mail people an adult has approved and the messages I send will be polite and sensible. I will not open any e-mails from people I do not know.
- I will never give out personal information, passwords or arrange to meet anyone.
- I will not use Internet chat rooms.
- I understand that the school may check my computer files and monitor the Internet sites I visit.
- I will only bring a pen drive in to school if I have been given permission.