B.W.P.S.
E-Safety Policy

Revised: October 2017

Introduction
Electronic Safety (E-Safety) encompasses Internet technologies and electronic communications. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

* Websites
* Learning Platforms and Virtual Learning Environments
* Email and Instant Messaging
* Chat Rooms and Social Networking
* Blogs and Wikis
* Podcasting
* Video Broadcasting
* Music Downloading
* Gaming
* Mobile/Smart phones with text, video and/or web functionality
* Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of Internet Technologies.

In Brackenagh West Primary School we understand the need to educate our pupils in E-Safety issues. We aim to teach them appropriate online behaviour, to enable them to remain both safe and legal when using the internet and related technologies, both in and beyond the context of the classroom.

The school's E-safety Policy should operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

Education of Pupils
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement & well being, and to support the professional work of staff and enhance the school's management information system.

Roles and Responsibilities
As E-Safety is an important aspect of leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

It is the role of the ICT Co-ordinator to keep abreast of current E-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of E-Safety throughout the school.

The Principal has the responsibility to update the Governors with regard to E-Safety and all Governors should have an understanding of the issues at involved.

Writing and Reviewing the E-Safety Policy
This policy, supported by the school's Acceptable Use Agreement for staff and pupils, is to protect the interests and safety of the whole school community.

E-Safety issues are included in the Child Protection, Health & Safety, Anti-Bullying, Discipline and ICT policies.

The E-Safety policy has been agreed by the Senior Management Team, Staff and approved by the Governors. The E-Safety policy and its implementation will be reviewed bi-annually.

E-Safety Skills' Development for Staff
All staff will receive regular information and training on E-Safety issues at staff meetings.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.

INSET may be used to help staff develop their own practices and support pupils in safe and responsible use of ICT.

New staff members will receive a copy of the E-Safety Policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.

All staff are encouraged to incorporate E-Safety into their activities and to raise awareness within their lessons.

Risk Assessment
In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material through our C2K filtering service.

However, due to the huge scale and linked nature of Internet content, it is not possible to give a complete guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for any material accessed, or any consequences of Internet access.

Methods to identify, assess and minimise risks will be reviewed regularly. The Principal and ICT co-ordinator will ensure that the Internet policy is implemented and compliance with the policy monitored.

Risks that may occur for learners include the following:

<u>Content</u>
* exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
* lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
* hate sites;
* content validation: how to check authenticity and accuracy of online content.

<u>Contact</u>
* grooming
* cyber-bullying

* identity theft and sharing passwords

Conduct
* privacy issues, including disclosure of personal information
* digital footprint and online reputation;
* health and well-being - amount of time spent online and for example the activity such as gaming or sexting (sending and receiving of personally intimate images)

School Website Content
• The point of contact on the website is the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

* Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by their full name. Teachers must be very aware of the following when choosing photos for the website:

- potentially embarrassing or distressing images will not be used;
- images that may be misused by others will not be used;
- the images will not be associated with sensitive issues; and
- the school will review and delete unwanted material.

* To reduce the risk of such images being used inappropriately, only images of pupils who are suitably dressed/posed will be used.

* Pupils' full names will not be used in association with photographs.

* Written permission from parents or carers will be obtained before photographs of pupils are used by the school.

Mobile Devices
* The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.

* Pupils' mobile phones are not permitted in school.

* In very exceptional circumstances this may be relaxed for a short period if a parent makes a request in writing to the Principal. In such instances the pupil's mobile phone will remain with his/her class teacher throughout the school day, and be returned to the pupil at home-time.

E-Safety Information for Parents/Carers
Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.

Parents/carers are required to make a decision as to whether they consent to images of their child being taken and/or used on the school website.

The school website contains useful information and links to sites like Net Nanny, Surf Watch, CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.

The school will communicate and promote relevant E-Safety information through newsletters and the school website.

Parents should remember that it is important to promote E-Safety in the home and to monitor Internet use.

* Keep the computer in a communal area of the home.

* Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.

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

* Take an interest in what children are doing. 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.

* Discuss the fact that there are websites/social networking activities which are unsuitable.

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

* Remind children never to give out personal information online.

* 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 and that this internet use may not be filtered or supervised.

Cyber-Bullying

Cyber-bullying is wilful and repeated harm (i.e., harassing, humiliating, or threatening text or images) inflicted through the Internet, interactive technologies, or mobile phones.

The responsibilities of the school and of pupils as set out in the Anti-Bullying Policy apply also to this policy.

We will seek to educate the children of the dangers caused by cyber-bullying, and they will be encouraged to report any such instances to their parents and/or class teacher.

Whilst education and guidance remain at the heart of what we do, Brackenagh West PS reserves the right to take action against those who take part in cyber-bullying.

* All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.

* Brackenagh West PS will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in or out of school.

* Brackenagh West PS will use its power of confiscation where necessary to prevent pupils from cyber-bullying or misusing equipment.

* All members of the School community are aware they have a duty to bring to the attention of the Principal any example of cyber-bullying or harassment that they know about or suspect.

Guidance for Pupils
If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent, your teacher, or the Principal.

* Do not answer abusive messages but report them
* Do not delete anything until it has been shown to your parent, your teacher, or the Principal.
* Do not give out personal details
* Never reply to abusive e-mails
* Never reply to someone you do not know

Guidance for Parents
It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying.

* Parents can help by making sure their child understands the school's policy and, above all, how seriously the school takes incidents of cyber-bullying.
* Parents should also explain to their children legal issues relating to cyber- bullying.
* If parents believe their child is the victim of cyber-bullying, they should save the offending material and make sure they have all relevant information before deleting anything.
* Parents should contact the school as soon as possible. A meeting can then be arranged, which may involve other relevant members of staff

Responding to cyber bullying
Cyber bullying will generally be dealt with through the school's Anti-Bullying policy. A cyber bullying incident might include features different to other forms of bullying, prompting a particular response.

Key differences might be:

* **Impact**: possibly extensive scale and scope
* **Location**: the anytime and anywhere nature of cyber bullying
* **Anonymity**: the person being bullied might not know who the perpetrator is
* **Motivation**: the perpetrator might not realise that his/her actions are bullying
* **Evidence**: the subject of the bullying will have evidence of what happened

We will keep records of cyber-bullying incidents to ensure consistency in our investigations, support and sanctions.

Communication about E-Safety
Parents' attention will be drawn to the School E-Safety Policy through letters home, information sheets and the school website.

Information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.

Internet issues will be handled sensitively to inform parents without undue alarm.

E-Mail
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.

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mails, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children are not always given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Internet Security
The Department of Education provides schools with the necessary hardware, software and connectivity to enable access to the Internet through an organisation called C2k. Access is thus controlled through a filtering mechanism controlled by C2k. However, no matter how thorough, a filtering service can never be comprehensive.

It is possible for unsuitable websites to become available, sometimes for short periods after they are launched. As soon as a site is deemed to be unsuitable, it will be blocked, so that no user can subsequently access it.

Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network solution.

Access to the Internet via the C2k Education Network is fully auditable and reports are available to the Principal.

Social Networking
The school C2k system will block access to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.

Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals. School staff will not add children as ‘friends’ if they use these sites.

Managing Video-conferencing
Video-conferencing will be via the C2k network to ensure quality of service and security, and will be appropriately supervised.

Password Security
Adult users are provided with an individual login username and password, which they are asked to change periodically. Login details should not be shared with pupils.

All pupils are provided with an individual login username and password.

Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.

Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

Bringing in Devices from Home
There may be occasions when pupils are allowed to bring iPads, laptops or other electronic devices into school. However, this is optional and is done entirely at their own risk. The school will not accept liability for any loss or damage incurred.

Handling E-Safety Complaints
Complaints of Internet misuse will be dealt with by a senior member of staff/SMT/ Safeguarding Team.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and reported to Safeguarding Team/SMT/Principal.

Any complaint about staff misuse must be referred to the Principal.

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.

Staff and the E-Safety Policy
All staff will be given the School E-Safety Policy and its importance explained.

Any information downloaded must be respectful of copyright, property rights and privacy.

Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.

A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software.

Staff can bring mobile phones, iPads, laptops and other electronic devices into school; this is done entirely at their own risk and the school will not accept liability for any loss or damage.

Monitoring and Review
This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the Governors' responsibility and they will review its effectiveness regularly.

Follow These SMART tips
Secret - Always keep your name, address, and password private.

Make sure you tell your parent or teacher if someone wants to talk to you when you are online.

Accepting e-mails or opening files from A people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

Remember that someone on-line may be lying and not be who they say they are.

Tell your parent if someone or something makes you feel uncomfortable or worried.