Kircubbin Integrated Primary School

E-Safety and Acceptable Use of the Internet and other Digital Technologies Policy.

Introduction

Online safety, in school and elsewhere, is of paramount concern. Schools play a crucial role in raising awareness of the risks, highlighting the impact of behaviour when engaging with online technologies and educating children and young people about how to act appropriately and stay safe. We want pupils to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other online. However, in doing so, they need to know how to protect themselves.

The Principal, Staff and Board of Governors will ensure that Kircubbin Integrated 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 phones and portable devices (e.g. iPads) which have downloadable capabilities.

What is E-Safety?

E-Safety is short for electronic safety. E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. 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. As a school we endeavour to promote safe and acceptable practices for all staff and pupils. This policy and its implementation will be reviewed annually by the I.C.T. Co-ordinator.

Potential Safeguarding Risks

In January 2014, the SBNI published its Report '*An exploration of e-safety messages to young people, parents and practitioners in Northern Ireland*.' The report points to a number of important factors which should be taken into consideration to minimise the potential risks around online safety. The report categorised the potential risks under four categories:

- **Content risks**: The child or young person is exposed to harmful materials.

- **Contact risks:** The child or young person participates in adult-initiated online activity and/or is at risk of grooming.

- **Conduct risks**: The child or young person is a perpetrator or subject to bullying behaviour in peer-to-peer exchange and/or is at risk of bullying, entrapment and/or blackmail.

- **Commercial risks**: The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs/fraud.

The Teacher's Role

In Kircubbin Integrated Primary School, staff are expected to, at all times, model and teach the safe and responsible use of ICT and the Internet. Furthermore, staff are asked to adhere to the school's guidelines on the use of social networking sites. Teachers are the first line of defence in E-Safety; 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. All staff will 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 and/or principal. This training will involve the sharing of age-appropriate resources and the latest guidelines on E-Safety as well as talks from local agencies such as the P.S.N.I.

Education of Pupils

The Internet is an integral part of pupils' lives, both inside and outside school. Kircubbin Integrated Primary School seeks to enable pupils to experience the benefits of communicating online with their peers, in relative safety. To achieve this E-Safety is discussed with pupils on a regular basis. This will take the form of age-appropriate lessons, Safer Internet Day and visits/presentations from local agencies such as the P.S.N.I. Use will also be made of resources from the Child Exploitation and Online Protection (CEOP), www.thinkuknow.co.uk and www.childnet.com. These activities will be incorporated into PDMU and ICT lessons. Through these activities:

- Pupils will receive age-appropriate online safety messages that are relevant and engaging.
- The school will promote online safety messages for pupils on how to stay safe; how to protect themselves online; and how to take responsibility for their own and others' safety.
- Pupils will be reminded to never to give out personal details of any kind which may identify them or their location on the internet.
- Pupils will know how to report an E-Safety problem.
- Pupils are informed that network and internet use will be monitored by the school and C2k.

Education of Parents and Wider Community

There are a number of useful guides and links on internet safety (including safety tips on specific social networking sites and gaming devices) available on the school website's 'Useful Links' section. Additionally, the school will also offer parents the opportunity to attend online safety training held by local agencies such as the P.S.N.I. The school will also promote online safety resources through publishing messages on the school's social media platform.

Cyber Bullying

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school.
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. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- 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 cyber-bullying can constitute a criminal offence. Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the School's Anti-Bullying and Discipline Policies.

If any user experiences or witnesses anything which they believe may be an e-safety issue they should report this to the school immediately.

Acceptable Use Guidelines

1. Conditions of Use

General

- Use of ICT in the Northern Ireland education community must be in support of the aims and objectives of the Northern Ireland Curriculum.
- All users must comply with all copyright laws.
- All users must limit their use of the Internet for school related purposes- examples of this include the use of email, the use of the Internet to investigate and research school subjects and staff using the Internet to further develop their professional development.
- All users are expected to behave in an appropriate manner when communicating with others.
- 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.
- All users must respect the hardware and software that has been made available to them.
- All users must respect the work of others.
- All Internet use will be accessed using the C2K network.
- All staff must ensure their passwords are not visible to others and must under no circumstances give their passwords out to anyone else.
- All staff should use the C2K email system as a means of communication. The C2K Network filtering solution provides security and protection to C2K email accounts.
- All staff should avoid social-networking with anyone under the age of 18. (See school Social Media Policy for more detail).
- In addition to this policy all staff, pupils and visitors must adhere to the school's mobile phone policy.

Pupils

- Pupils must not enter the folders or files of anyone else.
- Pupils must be aware that teachers have the right to enter any pupil's folder in their own class.
- The ICT Co-ordinator and Principal reserve the right to review files and communications of users to maintain system integrity and ensure that users are using the system responsibly - they will respect the right to privacy whenever possible.
- All pupils are responsible for their own behaviour on the Internet.
- Pupils must not deliberately seek out offensive materials. If pupils accidentally discover such materials they must tell the teacher immediately.
- Pupils must seek permission from the teacher before accessing the Internet.
- Pupils should not access other pupils' work unless they have been told to do so.

- Computers are only for school and homework use unless permission has been granted otherwise.
- Pupils must not use the Internet for unapproved purposes.
- Pupils who consistently choose not to comply with these expectations may be denied access to Internet resources.
- Pupils should be discouraged from bringing mobile phones and hand-held gaming consoles with downloadable capabilities to schools on the grounds that they :-
  -are valuable and may be lost or stolen.
  -are capable of storing images that are inappropriate.
- On an annual basis, parental permission is sought from parents before pupils access the internet.

Parents

- Parents should be aware that the access to the Internet provided to staff and children in school has limiting security features.
- Parents should be aware that the use of the Internet in school is closely monitored by staff.
- Parents should be aware that there will be no use of the Internet without the supervision of staff and that this will be in full view of others, e.g. the classroom or the ICT Suite.
- Parents should, in co-operation with staff, make children aware of the rules and expectations within this document.
- Parents should be aware that the use of ICT is complimentary to the teaching already done. i.e. the use of computers and iPads in the classroom is an additional educational tool.
- Parents should be aware that when photographs of pupils are used children's full names will not be available online at any stage.
- Parents should be aware that occasionally children's work will be celebrated on the school website or social media platform.
- Parent should be aware that no photographs of children will be available online without parents giving their permission.
- On an annual basis, parental permission is sought from parents for the use of their child's photograph.
- Parents should discourage children from bringing mobile phones to school on the grounds that Internet access becomes very difficult to police.
- Parents should also be aware that the social networking sites, such as Facebook and Instagram, adhere to strict 'over 13's' age policies. Other social networking and messaging sites/apps also have age restrictions.

Addendum

Network administrators 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.

2. Location and Supervision

Internet access for staff and pupils is a filtered service managed and maintained by C2K. Each individual will have a unique username and should not permit other people to use it. All passwords are updated once a term. All users must be aware that the school and C2K routinely track and record the sites visited, the searches made on the Internet and e-mails sent and received by individual users.

Internet access for pupils in school should be available only on computers and iPads that are in highly used areas of the school such as classrooms and the computer suite.

While using the internet at school, classes should always be supervised. It is important to recognise however, that internet access is very difficult to police and that each child's monitor screen or tablet cannot be watched at all times. Therefore, in all cases, pupils are reminded of their responsibility to use the internet appropriately and in line with school safety rules.

3. Examples of Acceptable Use

On-line activities which are encouraged include, for example;
• the use of e-mail and conferencing for communication between pupils and teachers, between teachers and between schools and industry;
• use of the Internet to investigate and research school subjects, cross-curricular themes and topics related to social and personal development;
• the development of pupils' competence in ICT skills and their general research skills.

4. School Website/Facebook Page

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.
- No images will be accompanied by pupil's full names.
- The website does not include home addresses, telephone numbers, personal emails or any other personal information about pupils or staff.

5. Advice for Parents

- Parents should be aware that the use of the Internet in school is filtered and closely monitored by staff.
- While in school, teachers will guide pupils towards appropriate materials on the internet. Outside school, parents or guardians bear the

same responsibility for such guidance as they would normally exercise with information sources such as television, telephones, movies, radio and other media.

- Parents should be aware that the use of ICT is complimentary to the teaching already done – i.e. the use of computers in the classroom is a tool.
- Parents should be aware that children's full names will not be available online at any stage. Photographs and examples of children's work, where permission has been given, may be posted on to the school website.

The guidance we give in school could be used at home and should include:

- Rules for safe use on the internet.
- Parents are encouraged to monitor their child's internet usage particularly with the upsurge in the use of social networking sites.
- Parents should ensure that they give their agreement before children give out personal identifying information.
- Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images.

Any parent or member of staff who wishes to discuss this document can put any questions to: -

Mr Irvine (Principal) or Mr Ferguson (ICT Co-ordinator)

This policy is based on "Acceptable Use of the Internet and Digital Technologies in Schools" (DENI Circular 2007/1 - 18 June 2007), eSafety Guidance (DENI Circular 2013/25 – 6 December 2013) and Online Safety (DENI Circular 2016/27 – 1 December 2016).

September 2019