BALLYORAN PRIMARY SCHOOL

E-Safety Policy

Reviewed April 2024

Introduction

In Ballyoran Primary School, we believe that the Internet and other digital technologies are important educational resources which when used appropriately and effectively, enhance learning and teaching.

This document sets out the Policy and Practices for the safe and effective use of the Internet in Ballyoran Primary School. The Policy applies to all members of Ballyoran Primary School including staff, pupils, parents/carers, visitors and community users who have access to and are users of school ICT systems, both inside and outside of school.

This Policy takes into account the following guidance:

- DENI Circular 'E-SAFETY Guidance' 2013
- DENI Circular 2016/27 Online Safety
- Safeguarding Board for Northern Ireland (SBNI) 2014

What is E-Safety?

In the school context E-Safety:

- Is concerned with safeguarding children and young people in the digital world.
- Emphasises learning to understand and use new technologies in a positive way.
- Is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online.
- Is concerned with supporting pupils to develop safer online behaviours both in and out of school.
- Is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

(DENI 2013)

The Education and Inspections Act 2006 empowers school Principals to such extent as it is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other E-Safety incidents covered by this Policy, which may take place outside of the school but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the Positive Behaviour Policy.

Ballyoran Primary School will deal with such incidents within this Policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate E-Safety behaviour that take place out of school.

How valuable is the Internet in Education?

The Internet is an exciting and unique resource. It brings the world into the classroom by giving children access to the global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow in the modern world. 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.

- It gives children opportunities to locate, retrieve and exchange information.
- It encourages the development of ICT skills that are vital to life-long learning.
- It takes learning beyond the classroom.
- It allows access to stores of information that might otherwise be unavailable in school.
- It provides up-to-date information.
- It is a fast and efficient way of communicating and retrieving information.
- It encourages independent learning.
- Children enjoy using it.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. 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 (live or edited)
- Music Downloading/Production
- Gaming
- Mobile/Smart phones/Smart watches with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.
In Ballyoran Primary School we understand the responsibility to educate our pupils in online safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

What are the dangers?

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials; some of which could be unsuitable. Key concerns are:

Potential Contact
Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons.

Children should be taught:

- That people are not always who they say they are.
- That 'Stranger Danger' applies to people they encounter through the Internet.
- That they should never give out personal details.
- That they should never meet alone anyone contacted via the Internet.
- That once they publish information it can be disseminated with ease and cannot be destroyed.

Inappropriate Content
Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content. Materials may express extreme views e.g. some use the web to publish information on weapons, crime and racism that would be restricted elsewhere. Materials may contain misleading and inaccurate information e.g. some use the web to promote activities that are harmful such as anorexia or bulimia.

Children should be taught:

- That the information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.
- Not to fill in forms asking for their personal details.
- Not to use an adult's credit card to order online products.

Excessive Commercialism
The Internet is a powerful vehicle for advertising. In visiting websites, and through online gaming, children have easy access to advertising that is very persuasive. If children are to use the Internet in places other than in school e.g. libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school.

Board of Governors
The Board of Governors is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of this policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports.

Principal

- The Principal has a duty of care for ensuring the safety (including E-Safety) of all members of the school community.
- The Principal and School Leadership Team will be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.
- The Principal is responsible for ensuring staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support for those in school who carry out the internal E-Safety monitoring role.
- The School Leadership Team will receive regular monitoring reports from the ICT/E-Safety Coordinator.
- The Principal uses Securus to monitor the screen display and keystrokes of pupils who may be at risk or in breach of acceptable use.

ICT/E-Safety Coordinators

- Takes day-to-day responsibility for E-Safety issues and has a learning role in establishing and reviewing the school E-Safety Policies and documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provides training, advice and liaise with staff.
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- Meet with the Principal to discuss current issues and review incident logs.

Teaching and Non Teaching Staff
Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable User Agreement.
- They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation.
- All digital communications with pupils, parents/carers and others should be on a professional level.
- E-Safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the E-Safety and Acceptable Use Policies.

- They monitor the use of digital technologies and mobile devices in lessons and other school activities and implement current policies with regard to these devices.
- In lessons were internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where lessons take place using live-streaming or video conferencing, safeguarding practices are followed.
- No filtering service is 100% effective, therefore all children's use of the Internet should be supervised by an adult.
- They model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Safeguarding Team
The Safeguarding Team are trained in E-Safety issues and are aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand School Policies on the use of mobile devices and on taking/use of images and cyber bullying.
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Pupils are not permitted to bring any mobile device, including mobile phones into school. If they do so, the device will be removed and Disciplinary Procedures may be followed.

Parents/Carers
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. It is important for them to promote Internet safety in the home and to monitor internet use. Ballyoran Primary School will take every opportunity to help parents understand these issues through news sheets via The School App, information on the school website, leaflets and E-Safety campaigns such as Safer Internet Day. Parents and carers will be encouraged to support the school in
promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to Parents' Sections of the school website
- Community Users

- Community users who access the school systems as part of the wider school provision will be expected to sign a Community Users Acceptable Use Agreement before being provided with access to school systems.

Education of Pupils

Pupils receive age-appropriate online safety messages that are relevant and engaging. The school actively promotes 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. Online Safety is taught as part of ICT.

Online safety is actively promoted within the school, for example through the development of online safety messages by the learners themselves, assemblies, participation in events such as Safer Internet Day and associated competitions organised by agencies such as EA/C2k.

- Pupils are taught in all lessons to be critically aware of materials and content they access on-line and the validity of the material they access.
- We use the filtering system on the server, as supplied by C2K which minimises the chances of pupils encountering undesirable material.
- Pupils are told to report to their teacher immediately if they access something which they believe is unsuitable or they feel uncomfortable with.
- Children are not permitted to use the internet during wet lunch/break times.
- Children's use of the internet is always supervised by an adult.

Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material. In school, we follow the **SMART** tips:

S – Secret – always keep your name, address, mobile number and password private.

M – Meeting – someone you have contacted through the internet can be dangerous. Only do so with your parent's/carer's permission and then when they can be present.

A – Accepting – accepting emails or opening files from people you do not really know or trust can get you into trouble, they may contain nasty messages or viruses.

R – Remember – remember someone online may be lying and not be who they say they are.

T – Tell – tell your parent or carer if someone or something makes you feel uncomfortable or worried.

(SMART Tips from: - Helping your parent be cool about the internet, produced by: Northern Area Child Protection Committees)

Internet use

- The school will plan and provide opportunities within a range of curriculum areas to teach Online Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them.
- Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies: i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question that has arisen from work in class.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

Managing Video-conferencing

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

Education and Training – Staff

We understand that it is essential that all staff receive E-Safety training and understand their responsibilities as outlined in this Policy. We educate our staff on E-Safety through:

- All new staff receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable User Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisation.
- The E-Safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

Technical – infrastructure/equipment, filtering and monitoring

- Ballyoran Primary School's network is managed by C2K, which provides filtering online
- C2K provides every pupil and member of staff with a unique username to access C2K services.
- User activity is logged and reports of usage are available to nominated staff within the school.
- Community users and visitors are given guest accounts in which their internet use is also filtered.
- Our wireless network is also managed and filtered by C2K.
- iPads are able to connect to the wireless network through a shared device account which is also filtered by C2K.
- Securus is used to monitor the screen display and keystrokes of pupils who may be at risk or in breach of acceptable use.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant access to images they have recorded themselves.

- In order for pupil images to be used on the school website written permission from parents or carers is obtained.
- We also educate pupils about the risks associated with taking, using and sharing images and the risks attached to publishing their own images on the internet.
- Any pictures taken using iPads are deleted by the user when they are no longer required and are only taken with the permission of the class teacher as they see it appropriate for pupils to do so.
- Teachers are not permitted to take photographs using their own mobile devices when in school or on educational visits outside school.

Social Media

Pupils

- Pupils do not have access to social media sites in school.
  Pupils are educated on the risks involved in using social media websites outside of school.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. **(See Appendix 1)** 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.

Staff

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.

Cyber Bullying
Cyber bullying can take many different forms and guises including:

- Email
- Instant messaging and Chat rooms
- Social Networking Sites
- Online Gaming
- Mobile Phones
- Abusing Personal Information
- Sexting

As a school, we are aware that pupils may be subject to Cyber Bullying via electronic methods of communication both in and out of school.

Considering this we take the following steps in relation to cyber bullying:

- Pupils are educated in recognising what Cyber Bullying is and reminded that it can constitute a criminal offence.
- They are reminded that whilst Cyber Bullying may appear to be anonymous for the bully, messages can be traced back to their creator.
- They are taught what to do if they are the receiver of bullying over the internet/mobile devices.
- They are told to inform a parent or teacher immediately and this will be reported to Senior Management.
- Cyber Bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Incidents will be dealt with using the school's Anti-Bullying and Positive Behaviour Policies.
- All incidents of Cyber Bullying reported to the school will be recorded
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

Email

- 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.
- Each member of staff has a unique e-mail address and password.
- Children do not have access to e-mails unless authorised to do so by the ICT Coordinators.

School Website

- Children are only referred to by their first names.
- Images of children will not be labelled with their name.
- No personal details will be given for any of the school community.
- Websites/Apps selected by teachers may be put on the website for pupils to access outside of school – sites/Apps will be previewed and checked regularly.
- Permission from parents/carers will be sought to publish work and/or photographs on the school website.

M**obile Technologies**

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer viruses and inappropriate material. All teachers have been provided with an encrypted USB memory stick.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to bring or use personal mobile devices/phones/ Smart Watches to school.
- Staff should not use personal mobile phones during designated teaching sessions.

Monitoring and Review

This policy is implemented daily and is monitored by the ICT Coordinators and Designated Teacher. This policy will be reviewed annually with the Safeguarding/Child Protection Policy.

Appendix 1

Ballyoran Primary School

CHILDREN'S USE OF SOCIAL MEDIA

Dear Parent/Guardian

As part of the school's ongoing, proactive approach to Internet Safety and the safe use of digital technologies, we would like to take this opportunity to draw parents'/guardians' attention to the following:

An increasing number of pupils are indicating that they have access to, or regularly use, social media platforms such as SNAPCHAT, INSTAGRAM, TIK TOK, WHAT'S APP and FACEBOOK. We would like to remind parents/guardians that these platforms are **AGE RESTRICTED** and **it is the view of the school that they SHOULD NEVER be used by any primary school aged pupil.**

It is the responsibility of parents/guardians to be ***fully aware*** of what their child is doing online. The school will not become involved in situations where pupils behave inappropriately on those platforms outside of school. Should instances of online bullying and abuse be reported to the school by concerned parents, we will advise those parents how to report the incident to the appropriate authorities. ***It is up to you to keep your child safe from internet bullying while at home***.

We suggest that you use the following 5 measures to ensure that you can monitor your child's mobile phone/tablet to ensure their safety:

(1) Agree that *you* can have access to their phone whenever you want; *check the phone regularly.*
(2) Make sure you *know what apps they are using* (age appropriate) and *know all their passwords* for these apps.
(3) Look at and *monitor the history of their calls, messages, contacts, web-site and pictures*.
(4) No child needs their phone after 8:30pm or before 8:30am….and definitely ***NO CHILD NEEDS HIS/HER PHONE IN THE BEDROOM AT NIGHT***.
(5) At all times *talk to your child regarding the dangers of social media*. Remember 1 out of 5 children talk to a stranger every day through social media.

This letter does not mean that we agree with your child having access to social media, as stated above we would advise against it but if you insist on letting your child use it, then this advice will hopefully help to keep them safe.

Yours Sincerely
Richard Woolsey
Principal

Check out:
www.ballyoranps.com/internet-safety
www.nspcc.org.uk/preventing-abuse/keeping-children-safe
www.thinkuknow.co.uk/parents