

BELLAGHY PRIMARY SCHOOL

E-SAFETY POLICY

1. SCHOOL ETHOS AND MISSION STATEMENT

Bellaghy Primary School strives to provide, in partnership with parents, a broad quality education so that all the pupils can reach their full potential within a caring, secure environment promoting self-discipline, motivation and individuality.

2. RATIONALE

Being online is an integral part of children and young people's lives in the 21st Century. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form a part of children and young people's online world.

The internet and online technology provide new opportunities for young people's learning and growth, but it can also expose them to new types of risks.

Government guidance for schools highlights the importance of safeguarding children and young online. E-safety forms a fundamental part of our school's safeguarding and child protection measures. Having a whole school approach helps ensure staff, governors, volunteers and parents teach children about online safety.

Our school has a dual responsibility when it comes to e-safety: to ensure the school's online procedures keep children and young people safe, and to teach them about online safety, in and outside of school.

We strive to foster an open environment in which children and young people are encouraged to ask any questions and participate in an ongoing conversation about the benefits and dangers of the online world.

3. LEGAL FRAMEWORK

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in Northern Ireland. Summaries of the key legislation and guidance are available on:

- Online abuse learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- Bullying learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- Child protection learning.nspcc.org.uk/child-protection-system

In devising this policy, reference is made to DE Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools.

4. KEY MESSAGES

We believe that:

Children and young people should never experience abuse of any kind.

Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

The online world provides everyone with many opportunities; however, it can also present risks and challenges.

We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online.

We have a responsibility to help keep children and young people safe online, whether or not they are using [name of organisation]'s network and devices.

All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children safe by:

- appointing an online safety coordinator – this will be our Designated Teacher for Child Protection,

- providing clear and specific directions to staff and volunteers on how to behave online through our Code of Conduct and Policy on Acceptable Use of Mobile Devices,
- supporting and encouraging children to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others,
- supporting and encouraging parents and carers to do what they can to keep their children safe online,
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person,
- ensuring that user names, logins, email accounts and passwords are used effectively,
- ensuring personal information about the adults and children in our school is held securely and shared only as appropriate,
- ensuring that images of children are used only after parental permission has been obtained, and used only for the purpose for which consent has been given,
- providing supervision, support and training for staff and volunteers about online safety.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our school as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

5. INTERNET USERS (both staff and children)

When using the Internet, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws, and all school staff (both teachers and non-teaching staff including volunteers) are expected to communicate in a professional manner.

Children must be responsible for their good behaviour on the school networks, as they should when off school premises. While the use of information and communication technologies is a required aspect of the statutory Northern Ireland Curriculum, access to the Internet remains a privilege and not a right. It is given to pupils who act in a considerate and responsible manner and should be withdrawn if they fail to maintain acceptable standards of use.

Staff ensure that pupils know and understand that no Internet user is permitted to:

- retrieve, send, copy or display offensive messages or pictures;
- use obscene or racist language;
- harass, insult or attack others;
- damage computers, computer systems or computer networks;
- violate copyright laws;
- use another user's password;
- trespass in another user's folders, work or files;
- intentionally waste resources (such as on-line time and consumables).

6. LOCATION AND SUPERVISION

At Bellaghy Primary School, we ensure that access to the Internet provided to staff and children is a filtered service through the C2K network. All users have access to PCs, laptops and ipads. All users are aware that the school can and does track and record the sites visited, the searches made on the Internet and e-mail sent and received by individual users.

Internet access for pupils in our school is available only on computers that are in highly-visible areas of our school such as classrooms. Machines which are connected to the Internet are in full view of people circulating in the area.

While using the Internet at school, pupils, where possible, are under supervision.

A poster explaining appropriate use of the Internet is displayed in each classroom. (See Appendix 1)

7. EXAMPLES OF ACCEPTABLE AND UNACCEPTABLE USE

On-line activities which are encouraged include, for example:

- the use of email and computer conferencing for communication between colleagues, between child and teacher, between pupil and pupil, 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 children's competence in ICT skills and their general research skills.

On-line activities which are not permitted include, for example:

- searching, viewing and/or retrieving materials that are not related to the aims of the curriculum;
- copying, saving and/or redistributing copyright protected material, without approval;
- subscribing to any services or ordering any goods or services, unless specifically approved by the school;
- playing computer games or using other interactive 'chat' sites, unless specifically assigned by the teacher;
- publishing, sharing or distributing any personal information about a user (such as: home address; email address; phone number, etc.);
- any activity that violates a school rule.

8. REMOTE LEARNING

When learning from home during an exceptional closure, children must follow the same standard of online behaviour as they would in school. The chosen platform for online use is Seesaw and parents must sign a Seesaw Consent form annually. This online platform will be used by staff and children for homework activities and for communication between school and home. (See Remote Learning Policy)

9. ADVICE FOR PARENTS

While in school, teachers will guide children towards appropriate materials on the Internet.

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

Appropriate home use of the Internet by children can be educationally beneficial, and can make a useful contribution to home and school work. It should, however, be supervised, and parents should be aware that they are responsible for their children's use of Internet resources at home.

10. GOOD PRACTICE FOR PARENTS

- parents should discuss with their children the rules for using the Internet and decide together when, how long, and what comprises appropriate use;
- parents should get to know the sites their children visit, and talk to them about what they are learning;
- parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud;
- 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.
- parents should be aware that the school cannot deal with any offensive online activity which occurs between pupils outside of school.

11. OUTSIDE AGENCIES/EVENTS

At regular intervals, the school will invite speakers from other agencies to speak to the children about e safety, e.g. P.S.N.I. or N.S.P.C.C.

The school will host seminars for parents on e safety.

The school will respond to specific e safety events e.g. Safer Internet Day.

The school will engage in frequent teaching and learning experiences on e safety as part of the preventative curriculum. These lessons will be whole school based (e.g. as part of an Assembly) and class based.

12. RELATED POLICIES

This Policy sits alongside many other policies within our Safeguarding Portfolio, including:

- Child Protection
- Anti-Bullying
- Positive Behaviour
- Pastoral Care
- Remote Learning Policy
- Staff Use of Social Media
- Staff Code of Conduct
- Staff Use of Mobile Devices
- Use of Mobile Devices in school
- Photography

POLICY UPDATED – November 2021 MLR

APPENDIX 1 – (displayed in each classroom)

BELLAGHY PRIMARY SCHOOL

RULES FOR RESPONSIBLE USE OF INTERNET

In our school, we have computers, laptops and iPads with Internet access to assist with our learning. These computers are fitted with built-in filters for our safety. Below are listed some rules which all users must adhere to. These rules will keep everyone safe and help us to be fair to each other.

- I will not access other people's files
- I will only use the computer for school work or for preparation for homework
- I will not bring in a device from home without permission from my teacher
- I will ask for permission before I use the Internet
- I will only visit sites approved by my teacher
- I will only e-mail people I know, or my teacher has approved
- The messages I send will be responsible and polite
- I will not give my home address or telephone or mobile number or arrange to meet someone unless my parent or teacher has given permission
- I will report any unpleasant material I come across on the Internet to my teacher
- I will report any messages sent to me
- I understand that my teacher can access my files and may monitor the sites I visit