Dungannon Primary School

Digital Safeguarding

Policy

Rationale

At Dungannon Primary School the Internet and other digital and information technologies are widely used in all classrooms as an excellent resource in supporting and enhancing the teaching and learning that is exciting. It also widens opportunities for children outside of the classroom and plays an ever-increasing role in their everyday lives. Whilst the use of the Internet and digital technologies present many positive and beneficial opportunities in and out of the context of education, all users must be made aware of the range of risks and challenges they may face when online. Dungannon Primary School recognises that digital safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Dungannon Primary School identifies that the risks online can be categorised into four main areas.

Content: Exposure to inappropriate or harmful content when online including sexual images, pornography, racist and hate content and information on suicide or self-harm.

Contact: Experiencing harmful interaction with other users including the grooming or exploitation of a child or young person for sexual, criminal or financial reasons.

Conduct: The behaviour of individuals when online that can cause harm such as online bullying, sharing or receiving inappropriate images or viewing or sending pornography.

Contact: Experiencing risk from online gambling, inappropriate advertising, phishing or financial scams.

The purpose of this digital safeguarding policy is to:

- ensure the safety of all pupils and staff when online.
- recognise approaches to teach and promote awareness of being safe online.
- support all staff to role model positive online behaviour and to display professional practice when online.
- identify the correct measures and actions to follow when responding to online safety concerns.

This policy considers statutory legislation and guidance and guidance including (but not limited to):

- The Department of Education Online Safety (2016)
- Education Authority
- Safeguarding Board for Northern Ireland Annual Report 2022-2023
- United Nations Convention on the Rights of the Child

The policy also has regard to the following non-statutory guidance including (but not limited to):

- NSPCC
- CEOP
- Childline

Links with other policies. This policy is linked with other policies including:

- Mobile phone policy
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- ICT Policy
- Positive Behaviour Policy

Roles and Responsibilities

- The Principal, Mr Thompson along with the Designated Teachers, Miss Wilson and Ms Hull and Deputy Designated Teacher Miss Leitch have overall lead over safeguarding in school, including online safety.
- The Principal and Board of Governors have the ultimate responsibility to ensure that the policy and practices are embedded and monitored.
- Dungannon Primary School recognises that all members of the school community must play an important role and show responsibility concerning online safety.

The Senior Leadership Team will:

- Ensure online safety practice is in connection with local and national guidelines and advice.
- Promote an online safety culture in a whole school setting.
- Support staff to embed online safety across the curriculum to ensure pupils develop an understanding of online safety.
- Work with staff to promote online safety.
- Ensure appropriate measures are in place for pupils and staff to report online safety concerns.
- Evaluate online safety practices within the school to identify strengths and areas for improvement.

The ICT Coordinator will:

- Develop and implement online safety policies and procedures that align with national guidelines and best practices.
- Educate and promote online safety to all students, staff and parents/carers.
- Take responsibility for implementing technical safeguards and appropriate filters to protect users from online threats.
- Monitor internet usage with the school to identify any potential risks or violations of online safety policies.
- Report incidents or concerns to the Principal and/or Designated Teachers.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT coordinator and recorded in the e-Safety incident logbook.
- Collaborate with all stakeholders to ensure that online safety is integrated into the curriculum and school culture.
- Liaise with staff to participate in events such as Safer Internet Day.
- Work closely with the Rights Respecting Schools Coordinator to promote the rights of the child.
- Meet termly with the Digital Leaders group to allow opportunities for opinions and concerns to be voiced and assist with them.
- Facilitate staff training on online safety.
- Keep up to date with current apps and online trends and disseminate information to staff and pupils.

Staff Members will:

- Be a positive role model for pupils by demonstrating respectful and ethical online behaviour.
- Incorporate online safety education into class activities and lessons across the curriculum.
- Supervise and monitor pupils' online activities to ensure the internet is used safely and appropriately.
- Promptly report any online safety concerns, such as cyberbullying, inappropriate content or suspicious online behaviour to the Safeguarding Team.
- Participate in online safety training sessions.
- Read and agree to the school's Acceptable Use Agreement (Appendix 1)
- Promote and Follow the Smart Tips (Appendix 3)

The Digital Leaders Group will:

- Serve as peer educators and provide support to their fellow students in understanding and practising online safety.
- Promote digital citizenship, which encompasses responsible and ethical behaviour online, such as being kind, and respectful and help them understand the impact of their online actions.
- Raise awareness of online safety.
- Promote online safety initiatives such as Safer Internet Day or assemblies led by the Steering Group on internet-related rights of the child.
- Provide peer support to their fellow students who may have experienced online safety issues.

- Collaborate with staff on integrating online safety education into class activities.

Parents and Carers

It is the responsibility of parents and carers to:

- Read through the Online Safety Policy and promote its values to their children.
- Read through and sign the Acceptable Use Agreement (see Appendix 2) on behalf of their child.
- Parents/carers are required to decide whether they consent to images of their child being uploaded on the school website and/or external agencies such as the local newspaper.
- Role model safe and appropriate use of the internet and social media.
- Promote and Follow the Smart Tips (See Appendix 3)

Teaching and Learning

Dungannon Primary School will raise awareness and promote safe and responsible use of online activity through:

- Ensuring our whole school approach is in line with Online Safety guidance from the Department of Education.
- Consolidate differentiated online safety education (suitable for the age and needs of the children) in all areas of the curriculum as appropriate and when online activities are used in lessons.
- Educate pupils on the dangers that may be encountered whilst online, and outside of school, and the importance of reporting risks and concerns.

- Ensure that pupils know who to report risks and concerns to such as parent/carer, teacher/trusted member of staff, designated teachers or an organisation such as Childline/CEOP.
- Promote online safety on national days such as Safer Internet Day.
- Encourage and promote the rights of the child in connection to internet use from the UN Convention of the Rights of the Child.
- Encourage children to be responsible for their digital well-being.
- Having a safe environment where children feel safe to be online and report concerns and issues.
- Inform children of the CEOP button and the details for Childline.
- Promote positive online safety activity with house points and praise.

Internet Use and Filtering

- C2k filters and monitors online activity.
- All users are aware that our system is monitored by C2k and the Principal will be made aware of inappropriate content.
- The Principal and ICT Coordinator have ensured appropriate filtering is in place to limit risk exposure.
- No filtering service is 100% effective; therefore, all children's use of the Internet is supervised by an adult.
- School tablets are not monitored by C2k. All pupils must be supervised to ensure they are completing the activity assigned by the teacher in a safe app or website.
- Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material. Online safety

rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start and throughout the year.

- Online activities are planned by teachers to encourage a focused use of the Internet. Children-friendly search engines are used to limit risk of reading inappropriate content.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Educated children that copying information directly from the internet may infringe copyright laws.
- Pupils should be taught to understand that not everything posted online is true.

School Website.

- Our school website address is www.dungannonps.co.uk.
- Teachers are responsible for uploading content to their class pages.
- The principal is responsible for verifying and making it live.
- The principal oversees uploading all other content to the school website such as policies, diary dates, holiday lists and other relevant information.
- School Web Design has the responsibility for the data and security of the school website.

Photos and Videos

- Only after written consent from parents/carers will photos and videos of their child be posted on the school website and or external agencies' websites.
- All photographs and videos uploaded to the school website will be appropriate and positive.
- Parents/carers may withdraw permission, in writing, at any time.

- Pupils' full names will not be displayed on the school website.
- Staff members will not take or store photos of pupils on personal devices.

Email

- All pupils and staff members have access to email through Office 365 using their C2k login details.
- Pupils are only permitted to use their C2k email address in school.
- Pupils must immediately tell a teacher if they receive an inappropriate e-mail.
- Pupils must not reveal personal details of themselves or others in e-mails.
- Emails sent in school for educational purposes will be supervised by a teacher.
- Staff and pupils must conduct themselves appropriately when communicating through email.
- The use of personal email addresses by staff for official school business is not permitted.
- Members of staff are encouraged to have a positive work-life balance when responding to emails from staff, pupils or parents.

Passwords

- All pupils and members of staff have a unique username and passwords to access the C2k system.
- All pupils and members of staff are responsible for keeping their passwords private.
- Staff members are required to use a strong password that is at least 11 characters long.
- All pupils and staff are asked to change their password every 70 days.
- All pupils and staff must never log in as another user.

- Lock devices or log off when leaving a workstation.
- The ICT coordinator has set up a sub-teacher account that all substitute teachers are required to use.

Remote Learning

- In the case of delivering lessons remotely, staff must continue to follow the Acceptable Use Policy.
- Ensure considerations of greater risks of one or both parties being in their own home and so both staff and pupils must ensure they are in an appropriate workspace and communicate with an appropriate code of conduct and professionalism.
- Due to the nature of remote learning, cameras and microphones may be active. Safeguarding and privacy policies must be followed, and personal information should not be discussed.
- Comment privately on the pupil's work, not in an open forum.
- If teachers are making videos as part of a lesson it must be filmed in an appropriate room with no other family member involved.
- In a live chat, staff must always have another member of staff present.
- Be available to respond to pupils between 9:00 am and 3:00 pm.
- Teachers must set work at the latest, by 3 pm on the day before the work is expected to be completed.

Social Media

- The C2k filter system will block access to social networking sites not available on C2k.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary-aged pupils.
- School staff will not add children as ‘friends’ if they use social media sites.
- If children are engaging in social media activities in school such as creating or contributing to a blog, bulletin board, or online forum, it will be done within the confines of C2k and will be filtered and monitored. They will be expected to conduct themselves positively and responsibly.

Mobile Devices

- All members of staff must store information and photographs of children on school iPads or C2k devices and not personal devices.
- Pupils are not allowed to use personal mobile devices/phones in school.
- If a pupil brings a mobile phone to school for safety purposes e.g. walking home from school, it must be switched off and stored in the central office during the school day.
- Pupils with smartwatches must never record or take a photograph of another child.
- Staff should not use personal mobile phones during designated teaching sessions.

Management of Online Safety Complaints

- Complaints of Internet misuse will be dealt with by the principal and/or designated teachers.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT coordinator and recorded in the e-Safety incident logbook.
- Any complaint about staff misuse must be referred to the principal.
- Complaints of a child protection nature must be dealt with following school child protection procedures.
- Pupils and parents will be informed of the complaint's procedure.

Monitoring

This policy is monitored regularly by the ICT Coordinator Due to the rapid changes in technology, this policy and its implementation will be reviewed annually by the Governors in liaison with the Principal, Safeguarding Team and the ICT Coordinator. This policy will be revised following any local or national policy updates.

Appendices

Appendix 1

Dungannon Primary School. Acceptable Use Agreement for Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- All Internet activity should be appropriate to staff professional activity or the pupils' education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied to letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

Signed:_____ Date: _____

Appendix 2

An Acceptable Use of the Internet for Pupils

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree on rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

· On the network, I will only use my login username and password.

· I will keep my username and password private.

· I will not access other people's files without their permission.

· I will not change or delete other people's work/files.

· I will ask permission before entering any website unless my teacher has already approved that site.

· I will use the Internet for research and school purposes only.

· I will only send an e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible.

· I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.

· When sending e-mail, I will not give my name, address or phone number or arrange to meet anyone.

· I understand that I am not allowed to enter Internet Chat Rooms while using school computers.

· If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.

· I will not bring in memory sticks from home to use in school unless I have been permitted by my class teacher.

· I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.

· I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.

· I understand that if I deliberately break these rules, I could be stopped from using the Internet/E-mail and my parents/carers will be informed.

Appendix 2 (continued)

DUNGANNON PRIMARY SCHOOL

Acceptable Use Agreement

For Pupils

Please complete and return this form to your child's class teacher.

Pupil's Name		Class Teacher	
As a school user of the Internet, I agree to follow the school rules on its' use. I will use the network in a responsible way and observe all the restrictions explained to me by my school.			
Pupil Name (print)			
Pupil Signature		Date	

Parents Name			
As the parent or legal guardian of the pupil above, I permit my son or daughter to use the Internet, including Email. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.			
Pupil Name (print)			
Pupil Signature		Date	

Appendix 3. Online Safety Poster for Classrooms.