

Donegall Road Primary School



E-Safety/Online Safety Policy

Date Ratified By Board of Governors: *December 2024*

Date of Review: *December 2025*

Staff Member Responsible: *Mr. Stringer (Acting ICT Co-ordinator)*

1. Introduction

1.1 School Ethos

In Donegall Road Primary School, all children are valued, nurtured and celebrated in a safe environment, where they are encouraged to succeed to the best of their ability and develop as citizens of the community.

1.2 Policy Context

This policy is based on and complies with the following documents:

- DENI Circular 2016/27 'Online Safety'
- DENI 'Safeguarding and Child Protection in Schools: A Guide for Schools' (updated September 2024)

In Donegall Road PS we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

The above circular, 'Online Safety', states that:

"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."

This document sets out the policy and practices for the safe and effective use of the Internet in Donegall Road Primary School. It will be approved by governors and available to all parents.

The policy and its implementation will be reviewed annually.

2. Definition of Online Safety

"Online safety means acting and staying safe when engaging in the online world. It is wider than simply internet technology and includes electronic communication via text messages, making comments on social media posts, social environments and apps, and using games consoles through any digital device. In all cases, in schools and elsewhere, it is a paramount concern." DENI Safeguarding and Child Protection in Schools: A guide for Schools (updated September 2024).

The UK Safer Internet Centre classifies risks as follows:

- **Content:** the child or young person is exposed to harmful material, for example pornography, racist or homophobic abuse, or pro-self-harm/suicide information.
- **Contact:** the child or young person is a victim of adult initiated online activity such as online grooming, harassment, sexual abuse or exploitation, extortion or ideological persuasion (radicalisation).
- **Conduct:** the child or young person is a victim or perpetrator of inappropriate or illegal peer to peer activity such as sexting, cyberbullying or sexual harassment.
- **Commercialism:** the child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs, such as online fraud or scams, in-app purchases, or illegal or age restricted products or services.

3. Roles and Responsibilities

3.1 ICT Co-ordinator

The ICT Co-ordinator will lead online safety and take day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school's policies and documents relating to online safety and acceptable use. They may delegate to ICT technical staff appropriate duties, such as carrying out health checks of the school's filtering systems.

The ICT Co-ordinator will:

- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide training and advice for staff as appropriate.
- Liaise with C2K and ICT technical staff.
- Liaise with the EA and DENI on online safety developments as appropriate.
- Receive reports of online safety incidents and create a log of incidents to inform future practice.
- Attend relevant meetings with the Board of Governors as appropriate.
- Discuss current issues with SLT and review incident logs.
- Monitor the curricular opportunities for implementation of online safety as part of the ICT curriculum.
- Consult with parents and outside agencies as appropriate in relation to online safety education.
- Ensure pupils and staff comply with the Acceptable Use Agreements and BYOD Policy (see Appendix).

3.2 Head of Pastoral Care/Designated Teachers for Child Protection

The Designated Teacher for Child Protection (and their deputy) will be trained in online safety issues as appropriate and be aware of the potential for serious child protection 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.

3.3 ICT Technical Staff

The ICT technician will work in consultation with the ICT Co-ordinator to ensure:

- C2K operates with robust filtering and security software.
- The school infrastructure and individual workstations are protected by up-to-date virus software by C2K.
- The school meets required online safety technical requirements, that users may only access the networks and devices through a properly enforced password protection policy in which passwords are regularly changed.
- The filtering policy is applied and to apply to C2K for any requests of sites to be unblocked.
- Software licences are accurate and up to date.

3.4 The Principal and Board of Governors

The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the designated members of staff. The Principal is responsible for appointing members of staff to act as C2K Managers.

The Principal and ICT Co-ordinator will be kept informed about online safety incidents.

The Principal and SLT are responsible for ensuring that the ICT Co-ordinator and other relevant staff receive suitable training and allocated time to enable them to carry out their online safety roles and to train other colleagues.

It is the responsibility of the Board of Governors to approve the Online Safety Policy and the Acceptable Use of the Internet agreement. They also must review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports from the Principal.

3.5 All School Staff

It is important that all staff realise and understand that they have the responsibility to ensure that:

- They have an up to date awareness of online safety matters and follow the current E-Safety/Online Safety Policy.
- They have read, understood and signed the Staff Code of Practice Acceptable Use Policy.

- They report any suspected misuse or problem to the ICT Co-ordinator or Head of Pastoral Care.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- They monitor ICT activity in lessons, extra-curricular and Extended School activities.
- Undertake all online safety training as organised by the school.

4. Code of Safe Practice

4.1 Acceptable Use Policy for Pupils

Pupil access to the Internet is through a filtered service provided by C2K, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents annually before pupils access the Internet.

In addition, the following key measures have been adopted by Donegall Road Primary School to ensure our pupils do not access any inappropriate material:

- The school's Code of Practice for use of the Internet and other digital technologies is made explicit to all pupils and is displayed prominently in suitable locations, such as the ICT suite.
- Our Code of Practice is reviewed each school year and signed by pupils/parents.
- Pupils using the Internet will normally be working in highly visible areas of the school.
- All online activity is for appropriate educational purposes and is supervised, where possible.
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group.
- Where the task involves pupils locating suitable websites themselves, explicit instruction will be provided by teachers of how best to locate appropriate sites, and how to evaluate their authenticity and appropriateness.
- Pupils in all Key Stages are educated in the safe and effective use of the Internet, through a number of selected programmes.

It should be accepted that however rigorous these measures may be, they can never be 100% effective. Neither the school, nor C2K, can accept liability under such circumstances.

4.2 Acceptable Use Policy for Staff

Staff are aware of the important role they play in promoting and protecting pupils' safe use of digital technologies. Each year members of staff using the school's ICT systems sign and agree to the Acceptable Use Agreement for Staff. Staff have also agreed that:

- Pupils accessing the Internet should be supervised by an adult at all times.
- All pupils are aware of the rules for the safe and effective use of the Internet. These are displayed in prominent locations within the school and discussed with pupils.
- All pupils using the Internet have written permission from their parents.

- Recommended websites for each year group have been approved by class teachers. Any additional websites used by pupils should be checked beforehand by teachers to ensure, as far as possible, there is no unsuitable content, and that material is age appropriate.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the ICT Co-ordinator.
- In the interests of system security, staff passwords should not be shared.
- Teachers are aware that the C2K My School system tracks all internet use and records the sites visited. The system also logs emails and messages sent and received by individual users. It is important that users are aware that a request may be made by the Principal to access such tracking information, and by signing the Acceptable Use Policy for Staff, members of staff authorise such information to be released to the Principal/Boards of Governors.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Staff understand that any work carried out on the C2k system whilst in the employment of Donegall Road Primary School remains the property of the school.
- Photographs of pupils should, where possible, be taken with a school camera and images stored on a centralised area on the school network, accessible only to staff.
- School systems may not be used for unauthorised commercial transactions.

5. Whole School Approach

In Donegall Road PS we believe that, alongside having a written E-Safety/Online Safety policy, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see the educational use of the Internet as an appropriate, effective, safe and essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. This policy outlines to all users (staff and pupils) what is safe and acceptable and what is not.

The scope of the policy covers fixed and mobile Internet; school PCs, laptops, iPads and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, iPads, tablets, Kindles) is subject to the same requirements as technology provided by the school.

C2k regularly monitor our network and ensures that the school meets recommended technical requirements.

The Wi-Fi for iPads is provided by C2k and filters are in place.

The I.C.T. Co-ordinator will monitor the effectiveness of the policy, particularly in the light of new developments in technology.

6. Education of pupils

We regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Online Safety Education for pupils. Rules for the 'Acceptable Use of the Internet' are discussed with all pupils. In addition, we take a preventive approach. Children follow a structured programme of age-appropriate messages regarding Online Safety Awareness in P.D.M.U. using a range of online resources e.g. <http://www.thinkuknow.co.uk/>. Outside agencies, such as NSPCC, Alternatives Justice Education and PSNI, are used to support Online Safety.

Pupil access to the Internet is through a filtered service provided by C2K, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

In addition, internet access on the iPads is the C2K Managed Network.

The following key measures have been adopted by Donegall Road Primary School to try to ensure that our pupils do not access any inappropriate material:

- Pupils using the Internet will normally be working in highly visible areas of the school.
- All online activity is for appropriate educational purposes and is supervised.
- Pupils will, where appropriate, use sites pre-selected by the teacher and appropriate to their age group.
- Pupils are educated in the safe and effective use of the Internet, through several selected programs.
- Pupils understand the importance of reporting abuse, misuse or access to inappropriate materials and know the procedures to follow. They are reminded of these during school assemblies.

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school, nor C2K, can accept liability under such circumstances.

The use of mobile phones/personal devices by pupils is not permitted on the school premises during school hours. All devices must be handed in to the class teacher or secretary on arrival at school for safe keeping. These can be collected again at the end of the school day.

Networking sites, besides 'MySchool', which is filtered and monitored by C2k, are not accessible for pupils.

Chatrooms, blogs and other social networking sites are blocked by the C2K filters and iPad wi-fi filters, so pupils do not have access to them in the school environment. Such communication is maintained within the educational learning environment on the C2K system (e.g. Just2Easy app). Pupils should not be on age inappropriate social networking websites outside of school.

7. Education of Staff

The ICT Coordinator will keep informed and updated on issues relating to Online Safety and attend courses when available. This training is then disseminated to all teaching staff, classroom assistants and supervisory assistants.

All teaching and non-teaching staff of Donegall Road PS are familiar with the Online Safety Policy. Safeguarding and Child Protection training will include online safety.

Staff members have agreed to the following guidelines of good practice:

- Staff share good practice in relation to online safety.
- Staff are aware that all digital communications with pupils and parents or carers should be on a professional level and only carried out using official school systems e.g. use of School Website, Facebook and See Saw app.
- Websites used by pupils should be checked beforehand by teachers where possible to ensure there is no unsuitable content and that material is age appropriate.
- Pupils accessing the Internet should always supervised by an adult. Content in screens should be visible to staff in the room.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- Staff discuss with pupils the rules for responsible internet use as pupils need to be taught how to be internet wise and learn how to recognise and avoid potential risks. Staff recognise that pupils need to know how to respond to inappropriate material.
- All pupils are aware of the rules for the safe and effective use of the Internet.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/I.C.T. Co-ordinator.
- In the interests of system security, staff passwords should only be shared with the network manager.
- Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- Photographs of pupils should, where possible, be taken with a school camera/iPad and images stored on a centralised area on the school network/password protected internet storage, accessible only to teaching staff. iPads are password protected.
- School systems may not be used for unauthorised commercial transactions.
- Staff should act as good role models while using digital technologies, the internet and mobile devices.
- Personal mobile devices should be switched off or on silent during the school day and kept out of sight.

8. Education of Parents/Wider Community

Parental permission, in writing, is sought for newly enrolled pupils to cover the use of photographs of pupils on the school website, Facebook, Seesaw app, in the local press and for displays etc. within school. It is the parent's responsibility to inform school of any changes in circumstances.

The Online Safety policy is available for parents to download from the school website or in paper format from the school secretary. Internet safety leaflets for parents and carers may need to be sent home when necessary. Parent awareness evenings may be organised and external agencies such as the PSNI may be asked to contribute.

If the school's I.C.T. facilities are used as a community resource under the Extended Schools programme, users need to be issued with separate usernames and passwords by C2K. They must also agree to the school's Acceptable Use of the Internet policy before participating and only access pre-selected and appropriate websites under the guidance of a tutor.

9. Monitoring and Evaluating

As part of our Safeguarding Policy, breaches of online safety are reported to the Designated Teacher for Safeguarding and Child Protection who records it and keeps any information secure.

The Online Safety Policy is reviewed annually or earlier if deemed appropriate. This could be because of recent online incidents or new circulars from the DENI.

The Online Safety Policy will be reviewed by the ICT Co-ordinator who liaises with the Designated Teachers for Safeguarding and Child Protection. If changes are to be made, staff are consulted.

10. Management of Personal Data

C2k regularly review and audit the safety and security of our school system. Servers, wireless systems and cabling is securely located, and physical access is restricted. All users have clearly defined access rights to school technical systems and devices. All users are provided with a username and secure password by the C2K Manager (ICT Coordinator) who keeps an up to date record of users and their usernames. Staff and pupils are responsible for the security of their username and password and will be required to change their password every 3 months.

Our school website 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. To minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions.
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area on the school network, or a password protected internet

storage facility, accessible only to teaching staff and technical staff of <http://schoolsupportni.com/>.

The Principal, School Secretary and ICT Coordinator are SIMS System Managers. They have access to the entire SIMS database. The managers can approve various staff access to the different modules within SIMS e.g. teachers have access to their class details, the assessment coordinator has access to all modules relating to assessment.

11.Reporting and Procedures

Donegall Road PS, in line with our Safeguarding and Child Protection Policy, has robust channels of communication in place for reporting online safety issues. Pupils and staff know who they can turn to if there is a problem. Instances relating to Safeguarding and Child Protection should be communicated to the designated teachers or principal. In cases of Internet abuse, or where a pupil is at risk, our safeguarding and child protection procedures will be implemented. Instances of cyber bullying of pupils or staff will be regarded as very serious offences.

The school will, if necessary; inform parents or carers of incidents of inappropriate Online Safety behaviour that takes place in our school.

Incidents of technology misuse which arise will be dealt with in accordance with the school's discipline policy. Minor incidents will be dealt with by the Principal/I.C.T. Coordinator and may result in a temporary or permanent ban on Internet use.

Appendix 1

Bring Your Own Device (BYOD) **User Agreement – Staff Declaration**

I request permission to use my personal ICT device in school.

Device Type: _____

Serial Number: _____

I have read and understood the Online Safety Policy and Acceptable Use Policy for Staff and I agree to be bound by all guidelines, rules and regulations contained within it. I agree to use the device for educational use only.

Disclaimer – please read carefully.

The school accepts no liability in respect of any loss/damage to personal ICT devices while at school or during school activities. The decision to bring a personal ICT device into school rests solely with the member of staff, as does the liability for any loss/damage.

I understand the disclaimer and accept that I am personally and solely responsible for the correct care, safety and security of the device. I understand that the school accepts no liability in respect of any personal ICT device used in school by a member of staff.

I understand that I may only connect to the school's filtered Wi-Fi networks once I have signed and returned this BYOD agreement and agree that I shall not try to circumnavigate or diminish the filtering security of the networks.

I am aware that the C2K My School system tracks all internet use and records the sites visited. The systems also log emails and messages sent and received by individual users and log all activity. It is important that users are aware that a request may be made by the Board of Governors, through the Principal, to access such tracking information, and by signing the Acceptable Use Agreement for Staff, members of staff authorise such information to be released to the Principal/Board of Governors.

This contract will remain in force throughout my time at school and it may be revised to take account of technological advancements in the interests of pupil and staff safety. Should I change my device, I agree to update this record with the ICT Co-ordinator.

Please complete and return this form to the ICT Co-ordinator.

Staff Name: _____

Signed: _____ Date: _____

Appendix 2

Acceptable Use of the Internet and Digital Technology for Pupils

Pupil Name: _____ Class: _____

Children should know that they are responsible for their use of the Internet and digital technology in school and that they must use it in a safe and appropriate manner. They must also realise that this agreement extends to the use of any technology or device on school premises, whether personally or school owned. Please discuss these guidelines with your child and stress the importance of the safe use of digital technology, including the Internet.

As the parent/guardian of pupil at Donegall Road Primary School, I agree that:

- They will take very good care of all equipment they use in school, treating it with respect.
- On the C2k network and any other appropriate apps, they will only use their own login username and password.
- They will keep their username and password private.
- They will not access other people's files without their permission.
- They will not change or delete other people's work/files.
- They will ask permission before accessing any website unless their teacher has already approved that site.
- They will use the Internet for research and school purposes only.
- They will only send e-mails in school when directed by their teacher using their C2K email account.
- They will make sure that the messages they send are polite and responsible.
- They understand that they are not allowed to access any private email accounts they may have whilst in school.
- They understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail or communicating digitally.
- When sending an e-mail, they will not give their name, address or phone number or arrange to meet anyone.
- They understand that they are not allowed to enter internet chat rooms while in school.
- If they see anything they are unhappy with or receive messages they do not like, they will tell a teacher immediately.
- They will not bring in memory sticks from home to use in school unless they have been given permission by the class teacher.
- They understand that the school may check their computer files/emails and may monitor the Internet sites that I visit.
- They understand that they must not use their mobile phone whilst on school premises. If they bring a phone to school, it must remain switched off and handed to their class teacher at the start of the day. The school accepts no responsibility for it should it go missing or get damaged.
- They understand that they should not bring wearable technology, such as smart watches, to school.

- They understand that they are not allowed to bring their own personal devices to school without the prior permission of the Principal/ICT Co-ordinator and that they must not try to connect any device to the school's networks.
- They understand that if they deliberately break these rules, they could be stopped from using the internet/e-mail/digital technologies, and that their parent/guardian will be informed, and sanctions will apply.
- They understand that the school computer/iPad systems log and monitor my use of the devices.
- They will use Seesaw safely and appropriately to showcase their achievements across the curriculum.

Parents/Guardians

As noted in the school's Online Safety and Acceptable Use Policy, both parents and staff have an important role to play in educating children on how best to use digital technology safely. As parents, it is important to seek to monitor and protect your child's online activity at home.

We all, parents and teachers, should remember that we are important role models in the lives of our children. We must all remember that any digital communication, such as social networks, are still subject to the rule of law. We must work together in partnership to educate our children and keep them safe online.

By signing below, you accept the above acceptable use agreement and consent to your child using Seesaw, noting the terms and conditions. More information is available at <https://web.seesaw.me/terms-of-service>.

Signature of Parent/Guardian: _____

Date: _____

Appendix 3

Acceptable Use Agreement for Staff

The computer system and associated digital technology 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 Acceptable Use Policy has been drawn up to protect all parties – the students, the staff and the school.

By signing this agreement, you recognise and accept that the Board of Governors reserves the right to examine or delete any files that may be held on its computer system, to monitor any Internet sites visited and to monitor and review the use of the school's digital technology.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the ICT Co-ordinator. By signing, members of staff accept and agree that:

- All Internet activity and use of digital technology should be appropriate to staff professional activity or the pupils' education.
- Access should only be made via your given authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school's ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail 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.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden and could be reported to the Police.
- When using school's social media accounts all posts and activity must be appropriate and acceptable, reflecting the ethos and values of the school.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Staff understand that any work carried out on the C2k system whilst in the employment of Donegall Road Primary School remains the property of the school.
- Photographs of pupils should, where possible, be taken with a school camera and images stored on a centralised area on the school network, accessible only to staff.
- School systems may not be used for unauthorised commercial transactions.
- Members of staff agree to maintain the confidentiality of records and information held digitally within the school, insuring they meet the requirements of the GDPR and the Data Protection Act.
- Staff should not be directly connected on social media to pupils at the school. They should also ensure that their social media does not give cause for the school to be called into disrepute.
- Staff should not use mobile phones in the presence of children within classrooms. During the teaching day, mobile phones should remain out of sight from children, unless

authorised by the Principal. Staff should, as far as possible, seek to use their mobile phones in the staffroom or office away from pupils.

- Staff accept that they may not connect personal devices to the school's C2k Wi-Fi network without accepting and returning to the ICT Co-ordinator a form of agreement to the school's Bring Your Own Device agreement.

Teachers are aware that the C2K My School system tracks all internet use and records the sites visited. The systems also log emails and messages sent and received by individual users and log all activity. It is important that users are aware that a request may be made by the Board of Governors, through the Principal, to access such tracking information, and by signing the Acceptable Use Agreement for Staff, members of staff authorise such information to be released to the Principal/Board of Governors.

Name: _____

Signed: _____

Date: _____