

**Online Safety Policy**

**Date: November 2021**

**Date of Review: November 2023**

**ETHOS**

The Drelincourt School provides a safe and happy environment where every pupil can develop to the very best of their ability. We want each child to remember this school as a happy place where they were nurtured, valued and inspired:

‘A little school for little people’

We have a responsibility for the safeguarding and child protection of the children in our care and we will carry out this duty by providing a caring, supportive and safe environment, where each child is valued for his or her unique talents and abilities, and in which all our young people can learn and develop to their full potential. This policy aims to provide Online Safety education which will safeguard and provide awareness to enable users to manage their experiences when using internet and related communication technologies.

This policy is based on and complies with DENI Circulars:

2011/22, 2013/25 and 2016/27 on **e-Safety**

2016/26 on **Effective Educational uses of Mobile Digital Devices**

2007/1 on **Acceptable use of the Internet and Digital Technologies in Schools**.

2015/21 on **School obligations- Information Governance and C2K Access to SIMS** 2018/08 on **The General Data Protection Regulation (GDPR) for Schools**

The circulars above state that:

*“Online safety, in all cases in schools and elsewhere, remains a paramount concern. It is essential not only that pupils and adults are kept safe online whilst in school and on school-organised activities, but that schools are energetic in teaching pupils how to act responsibly and keep themselves safe in the digital world.”*

**INTRODUCTION**

Online safety encompasses internet technologies and electronic communications such as computers, iPads, mobile phones and other portable digital devices.

Online safety relies on effective practice at various levels:

* Responsible use of ICT by all staff and pupils
* Thorough implementation of the online safety policy.
* The provision of a safe and secure internet network with monitored filtering system through C2K

**CARE AND RESPONSIBILITY**

Digital technologies are powerful tools that open up opportunities for everyone and have become integral to our lives. Children, staff and volunteers have a right to safer internet access at all times. The use of these new technologies can put users at risk. Some of the dangers may include:

* Access to illegal, harmful or inappropriate images or other content
* Loss of privacy / control of personal information
* Grooming by those with whom they make contact on the internet.
* The sharing / distribution of personal images without an individual’s consent or knowledge
* Inappropriate communication / contact with others, including strangers.
* Online-bullying
* Access to unsuitable video / internet games
* An inability to evaluate the quality, accuracy and relevance of information on the internet
* Plagiarism and copyright infringement
* Illegal downloading of music or video files
* Hacking, viruses and system security
* The potential for excessive use which may impact on children’s social and emotional development and learning.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other policies (e.g. safeguarding / child protection policies). As with all other risks, it is difficult to eliminate the risks completely. By providing good examples/role models and by raising awareness, it is possible to build the resilience of children, so that they have the confidence and skills to deal with these risks.

We have a significant role to play in keeping children safe and that includes online. Whether we provide internet access or not, young children will usually have access to the internet at home and we need to ensure their safety and well-being wherever they are.

Much of the current legislation that requires us to effectively safeguard children and users now includes clear references to online harms and online abuse. When defining “abuse”:

*“Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults, or another child or children.”*

**ROLES AND RESPONSIBILITIES**

Whilst it is primarily the duty of the Principal and the Board of Governors to ensure that the policy is in place and monitored, in practice all staff are involved as we are a small team. Staff work together under guidance of ICT Coordinator to keep abreast of current online safety issues and guidance through organizations such as CEOP (Child Exploitation and Online Protection), Childnet and Safer Schools NI App.

**ONLINE SAFETY AND STAFF**

### All staff are responsible for ensuring that:

* they have an up to date awareness of the online safety policy and practices
* they have read, understood and signed the staff/volunteer acceptable use agreement (AUA)
* understand and follow the procedures for reporting and recording online safety
* digital communications with children and families are professional *and only carried out using the official systems of the school.*
* young people in their care are aware of online safety
* they are aware of current online safety trends and issues (Safer School’s NI App)

**ONLINE SAFETY AND PUPILS**

###  Children

* are expected to abide by Buddy’s Internet Safety Rules ***(Appendix 1 and 2)***
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* should demonstrate positive online behaviours

Online safety will be discussed with all pupils at regular intervals throughout the school year. Activities will include teacher-led lessons and activities and lessons through outside agencies such as those for Safer Internet Day, DigiDuck Stories, Clickin Chicken and Buddy the Dog, and visits from local PSNI community team. The Teach Hub of the Safer School’s NI App provides access to lessons and stories that can be used.

**ONLINE SAFETY AND PARENTS**

### Parents/carers

Parents/carers play a crucial role in supporting their children in the use of good online safety practice.

* Parents/carers should discuss with their child and sign the acceptable use agreement
* Parents should sign Internet Use Agreement ***(Appendix 3)*** on behalf of their child
* Parents should sign digital/video images permissions, use of data permissions etc ***(Appendices 5 and 6)***

The Online Safety policy will be made available to download on the school website and a quick Parent Guide will be sent home and parents are asked to read this along with the other important school policies. Online safety will be promoted to parents via the school website and visits / talks from outside agencies such as the PSNI. Parents will be made aware of useful internet Online-Safety sites such as CEOP and thinkuknow through links on the website. The School has recently launched the Safer Schools NI App and this will become the main tool for parent/school online safety communication and information.

**TEACHING AND LEARNING**

**Internet use:**

* Teachers will plan and provide opportunities within a range of curriculum areas to teach Online Safety. The Safer Schools NI App is used to inform current practice and issues.
* Key messages will be reinforced regularly throughout the school year. These will be tailored to the level our pupils are at.
* Educating pupils on the dangers of technologies that may be encountered outside of school will be done informally and at a level which is appropriate for the pupils in our school.
* Pupils will be made aware of the impact of online bullying and how to seek help if these issues affect them.
* Pupils will be made and kept aware of where to seek advice or help if they experience problems when
* using the internet or related technologies; i.e. parent or guardian, teacher / member of the safeguarding team / trusted member of staff.
* School Internet access is filtered through the C2K managed service and any use of the internet is part of planned activities and will be monitored by an adult at all times.
* Pupils will be taught what acceptable use of the internet is, and will be helped to understand and act in accordance with the Acceptable Use Agreement.
* Pupils will be taught to be “Internet Wise”. They will be made aware of Buddy’s Internet Safety Rules and encouraged to discuss what to do should they come across inappropriate material.
* The school will ensure that the use of Internet derived materials by staff and pupils complies with the copyright law.
* Staff will act as good role models in their own use of ICT.

**ONLINE SAFETY DURING PERIODS OF REMOTE LEARNING AND/OR SCHOOL BASED VIDEO LESSONS**

In order to ensure the safety of all involved the following guidance should be followed if staff and pupils are engaging in online teaching/communication using digital platforms e.g. Seesaw, Zoom and Teams recommended by and available via C2K.

Live zoom lessons are always with the teacher in the classroom and links are checked regularly. Only known educational contacts are used for live lessons i.e. Museums on the Move, PSNI Santa Zoom, Neuronimo mood sessions, Amma Centre collaborations and Into Film.

On Seesaw children can only access lessons and activities prepared by the teacher. If there are videos used to aid understanding these are embedded using VideoLink to remove ads and potential for inappropriate content.

When teachers are recording lessons for Seesaw they are mindful of location and dress.

**•Parents and carers must set age-appropriate parental controls on digital devices and use internet filters to block malicious websites, as detailed in our Online Safety Policy. These are usually free, but often need to be turned on.**

**DIGITAL AND VIDEO IMAGES OF PUPILS**

As the school website continues to grow, it is intended that it will be used increasingly to exhibit the excellent learning and teaching that goes on in The Drelincourt.

The use of digital and video images of pupils will only be with written permission received from Parents / Guardians at the start of each school year. Permission can be withdrawn at any time in writing. Each consent form will be valid for one school year. Pupils’ full names will not be used on the website in association with photographs.

Teachers will take digital and video images of pupils and / or their work for observation and assessment purposes. Staff are aware that these images will be used solely for these purposes.

## PERSONAL DATA- PROTECTION

Personal data in our school is recorded, processed, transferred and made available according to the current GDPR data protection legislation

The Drelincourt School:

* has a Data Protection Policy
* implements the data protection principles and is able to demonstrate this through use of policies, notices and records
* has paid the appropriate fee to the Information Commissioner’s Office (ICO)
* has appointed an appropriate Data Protection Officer (DPO)
* we know and record what personal data we hold, where this data is held, why and which member of staff/volunteer has responsibility for managing it
* will hold only the minimum personal data necessary to enable us to perform our function and will not hold that data for longer than necessary for the purposes for which it was collected and always in accordance with our retention and disposal of records policy.
* provides staff and parents with information about how we look after their data and what their rights are in a clear Privacy Notice
* understands how to share data lawfully and safely with other relevant data controllers
* ensures that all staff receive data protection training at induction and appropriate refresher training thereafter

**NETWORKS**

All school ICT devices access the internet through the carefully filtered C2K system. Pupil’s access to the internet is monitored and supervised at all times. Where necessary pupils will access the internet through a child friendly, filtered search engine such as **kiddle.co.** Children have access to Junior Newsdesk on the C2K homepage and this also allows them to post comments in a safe and managed environment.

**E-MAILS**

The C2k Network filtering system provides security and protection to C2k email accounts. The filtering system offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content. Pupils will only experience C2K e-mail accounts on the school system as a group / class, and are not given individual e-mail accounts. E-mails sent and received as group / class activities will be supervised by staff at all times. Staff will only use C2K email accounts as a form of communication within the school and with outside agencies regarding school related business.

**SCHOOL WEBSITE**

The website is used to promote and provide up-to-date information about the school and showcase aspects of school life. In order to minimize risks of pupil or staff information on the website being used inappropriately the following steps are taken:

* Contact details on the website are the school address, info@email, telephone. No other personal information belonging to the staff or pupils will be published.
* Pupil’s names will be used infrequently and never in association with photographs.
* Access to loading pupil content on the website is restricted to teachers.

**SOCIAL NETWORKING**

## Social Media and Communications

At The Drelincourt we use a range of online services to communicate with our community, that include:

* Website messaging
* Social media pages - Twitter and Facebook
* Social media messaging
* Text messaging - Text Local
* Online portal pages e.g. Seesaw
* Email

All communications take place through clear and established systems and will be professional in nature. All staff have had clear, regularly updated guidance on their own use of personal media to protect their own professional role and the reputation of our setting.

The school has a Facebook and Twitter account for the purpose of school promotion and sharing of news and important information. This is not accessible to the children or used by them, it is a staff/parent/community tool. Social networking sites are blocked by the C2K filtering system. Staff who make personal use of social networking sites outside of school to promote the school should only reshare what is already on the school Facebook or website.

The use of pupil social network spaces is inappropriate considering the age of our pupils. However, through online safety lessons pupils will be encouraged not to give out personal information and to report any incidences to a trusted adult. If staff or pupils discover unsuitable sites while on the C2K system, the URL/website must be reported to a member of the ICT team or principal.

All communications take place through clear and established setting systems and will be professional in nature. Communications are monitored for concerns/complaints. There are clear processes in place to respond and resolve complaints or comments concerning our setting or staff/volunteers

**MOBILE TECHNOLOGIES**

Staff use of mobile phones should be discreet and never in the direct presence of pupils. During teaching time devices should be switched off/on silent and kept out of view. Personal devices are not generally used to take photos of children unless there is a specific reason i.e. better camera, issues with iPads, sending to Twitter. But this is always when multiple staff are present and aware. Pupils are not permitted to bring mobile phones into school.

Memory sticks are not needed within school but may on occasion be used by visiting speakers and/or substitute teachers. In accordance with GDPR regulations pupils’ personal data and images should not be stored on unprotected personal memory sticks, and should not leave the school premises.

**POLICY DECISIONS**

The school makes use of the 360 Early Years self audit tool for evaluating practice in online safety and considering targets for further development. The current audit and certificates are in the attachments.

**Authorising Internet Access**

The school will maintain an up to date record of all staff and pupils who are granted internet access through the C2K system and / or portable ICT devices. All staff must read and sign the Acceptable Use Policy before using any school ICT resource ***(Appendix 4).*** In all year groups access to the internet will be through well planned demonstrations or with direct supervision, with the aims of the lesson clearly stated and understood.

Parents and / or pupils will be required to sign and return a consent form agreeing to comply with the Acceptable Use Policy.

**PASSWORD SECURITY**

All staff are provided with individual login usernames and passwords are changed periodically when prompted by C2K. Staff should never share login details with anyone.

All pupils are provided with individual pin codes for logging on to the C2K network.

Staff Areas / Folders are the individual responsibility of each member of staff who must ensure they protect the security and confidentiality of the school network.

**HANDLING ONLINE-SAFETY COMPLAINTS**

Complaints of internet misuse will be dealt with by the ICT co-ordinator and Principal. Deliberate access to any inappropriate material by any user will be reported directly to the Principal.

Any complaint about staff misuse must be reported to the Principal.

Complaints of a child protection nature must be dealt with in accordance with the school Child Protection Policy.

Pupils and Parents will be informed of the complaints procedure.

**MONITORING, EVALUATION AND REVIEW**

This policy will be monitored and reviewed in line with the school’s policy review schedule.

**Appendix 1** 

Buddy’s Online Safety Rules for Children

**Internet Safety Rules**

1. Always ask a grown-up for help if you see anything strange or

 unusual.

2. Don’t download or install anything without asking a grown-up first.

3. Remember, not all games and videos are for children.

4. Don’t talk to strangers online and don’t tell them where you live.

5. If you are ever unsure what to do, remember Buddy’s song, and

 always ask for help.

**Appendix 2**

**Buddy’s ‘Use Your Tablet Safely’ Song**

(Sung to the tune of Frère Jacques)

Ask your grown-up, 

Ask your grown-up,

Ask for help!

Ask for help!

Use your tablet safely,

Use your tablet safely,

 Woof, woof, woof!

 Woof, woof, woof!

**Appendix 3**

***Under 5’s checklist for parents***

**START** setting some boundaries now – it’s never too early to do things like set limits for the amount of time they can spend on the computer

**KEEP** devices like your mobile out of reach and make sure you have passwords/PINs set up on them for the times you might lend them to your child... or for when they simply get hold of them themselves!

**CHECK** the age ratings and descriptions on apps, games, online TV and films before downloading them and allowing your son or daughter to play with or watch them

**EXPLAIN** your technology rules to grandparents, babysitters and the parents of your child’s friends so that they also stick to them when they’re looking after your child

**REMEMBER** that public Wi-Fi (e.g. in cafés) might not have Parental Controls on it – so, if you hand over your iPad to your child while you’re having a coffee, they might be able to access more than you bargained for

**SET** the homepage on your family computer or tablet to an appropriate website like CBeebies

**Reference:** http://www.vodafone.com/content/parents/get started.htm

**Appendix 4**

**ACCEPTABLE USE AGREEMENT FOR STAFF**

All users should have an entitlement to safe online access at all times.

This Acceptable Use Agreement is intended to ensure that:

* All staff will act responsibly to stay safer while online, being a good role model for children.
* effective systems are in place for the online safety of all users and the security of devices, systems, images, and data.
* staff are aware of and can protect themselves from potential risk in their use of online technologies.

**For my professional and personal safety, I understand that:**

* My use of technology could be monitored.
* When communicating professionally I will use the technology provided by the school (e.g. computers, laptops and i-pads). I will not use my own personal device, email address or social networking sites to take photographs of children or make contact with parents.
* These rules will apply when using the school’s technology eg. i-pads, either at home or away from the setting.
* I will only use the school’s technology for personal use with permission.
* I will only access, copy, remove or otherwise alter other user’s files, with permission
* I will communicate with others in a professional manner.
* I will only share other’s personal data with their permission.
* I understand that any images I publish will be with the owner’s permission and follow the school’s code of practice.
* I will only use the school’s equipment to record images of children

28

* I will only access materials and content that are legal and appropriate
* I understand the school’s reporting procedures and will immediately report any illegal, harmful or inappropriate incident.
* I will protect my online personal information (e.g. social networking profiles) to prevent access by the school’s children and families
* I will respect and follow any systems designed to keep the group safer

29

* personal passwords and those of other users should always be confidential.
* I will only download content that I have the right to use.

**ACCEPTABLE USE AGGREEMENT FOR STAFF - INTERNET STREAMING**

29

Through the C2k service, categories of sites can be made available to users, while access to other categories will be restricted. Access to the most inappropriate sites will always remain blocked.

We can choose to make users members of one or more internet related security groups as follows:

* Internet Social Networking
* Internet Streaming Media
* Internet Advanced

Access to these groups is controlled by the C2k Manager who can add individual users or groups of users to these groups via the Identity Management tool in MY-SCHOOL.

**Internet Streaming**

This group provides access to YouTube, BBC iPlayer, Vimeo and other television and radio streaming sites. When a user is added to the Internet Streaming security group the following categories, RED in the Default policy, are now GREEN. If a member of staff is to be added to the Internet Streaming groups they must agree to the following:

* To check all videos that are to be shown to classes before use
* Be responsible for the content of any video shown to a class

I agree to the terms of the Internet Streaming Acceptable Use Agreement and wish to be added to this group.

Staff signature: Date:

**Appendix 5** 

# Internet Use Agreement

A copy of Buddy’s Internet Safety Rules (guidance used in school for children) is attached to this permission form, so that parents/carers will be aware of the school’s expectations of the children in their care.

Parent/Carers Name:

Name of Child

As the parent/carer, I give permission for my child to use the school’s technology and devices.

I know that the school has made my child aware of Buddy’s Internet Safety Rules and has received guidance to help them understand the importance of online safety.

I understand that the school will take reasonable precautions to ensure that my child will be safer when online, however, I understand that this manages risk but cannot eliminate it.

I understand that my child’s online activity will be supervised and monitored and that the school will contact me if they have concerns about any possible breaches of the Internet Use Agreement.

I understand that the school will take appropriate action in the event of any incidents.

I will encourage my child to adopt safe use of online technologies.

**Signed Date**

31

**Appendix 6**

#

#

#

# Parental Guidance on use of Digital/Video Images

The use of digital/video images plays an important part in our activities. Children, staff and volunteers may use devices to record images/evidence of those activities. These images may then be used in Learning Journeys and presentations and may also be used to celebrate success through their publication in newsletters, on the website and occasionally in the public media.

*Our setting also uses CCTV to protect premises and our setting community. We ensure that these systems meet statutory and safeguarding requirements and the data recorded by these systems is compliant with the Data Protection Act 2018. There is clear signage indicating that CCTV is in use.*

The school will comply with the Data Protection Act and request parent’s/carers permission before taking images of their children. We will also ensure that, wherever possible, full names will not be published alongside images.

*It’s a great thing to film your child at our events and we know they provide a lot of precious memories. You can support us in keeping the children safe by considering the following:*

* Images and video should be for your own or family’s personal use only
* Think about privacy and who has the right to see your images, not only of your own child but of others
* If you do share the images online, then you must make sure they are limited to immediate family only and are not made public
* If you need help in knowing how to do this, then come and have a chat with us



**March 2022**

The named Staff members have access to the following internet platforms through the C2K Network:

* Internet Social Networking
* Internet Streaming Media
* Internet Advanced

Mrs E Trew (Principal)

Mrs S Walker (Teacher)

Miss J Tedford (Sub Teacher)

Mrs L McIlrath (Secretary)

Mrs S Ritchie (C/Assistant)

Mrs A Whitside (C/Assistant)