Dundela Infants' School and Nursery Unit

E-Safety Policy

Date issued – November 2021
Date of review – November 2023

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 whist 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

E-safety is short for electronic safety. It encompasses internet technologies and electronic communications such as computers, iPads, mobile phones and other portable digital devices.

The need has been highlighted to educate pupils, staff, Board of Governors and Parents about the benefits and risks of using technology. At Dundela we aim to provide an e-Safety education which will safeguard and provide awareness to enable users to control their experiences when maneuvering through the world of ICT.

E-safety relies on effective practice at various levels:

- Responsible use of ICT by all staff and pupils; encouraged by education and made explicit through school policies.
- Thorough implementation of the e-safety policy.
- The provision of a safe and secure internet network with a monitored filtering system.

Care and Responsibility

New technologies and the internet are an essential element in today's modern society, both within and outside school. Whist these are powerful tools and open up vast opportunities for learning, all parties making use of these tools should be made aware of the possible risks that can occur.

The use of ICT within school and at home has been shown to raise educational standards and promote pupil achievement.

However, with the use of these technologies there is also the possibility of some of the following risks:

- Illegal downloading of files- music / video / published works.
- The potential for excessive use which may impact on social and emotional development and learning.
- Unauthorized access to / loss of / sharing of personal information.
- The sharing / distribution of personal / another person's images inappropriately and / or without proper consents.
- Access to inappropriate video / internet games.
- Access to inappropriate / harmful / illegal images or content.
- Inappropriate communication / contact with others, including strangers.

- Being a victim / part of cyber-bullying.
- Social media- misuse / use of, that is not age appropriate
- Breach of personal data / conflict with the current GDPR guidelines

As with any other area of school life it is impossible to eliminate all risks completely. It is therefore our aim to help pupils, parents and staff equip themselves with the skills necessary to stay safe in this area.
This will be done through good educational provision to build awareness and resilience to the risks to which they may be exposed. This will allow the community of Dundela Infant's School to deal with any scenarios which may arise with confidence and knowledge.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership, Safeguarding and Child Protection within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are well known, understood, embedded and monitored.

It is the role of the ICT Coordinator, Mrs. E Yau, to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT co-ordinator and ICT team have responsibility for leading and monitoring the implementation of e-safety throughout the school.

The Principal and ICT Coordinator have the responsibility to update the Senior Leadership Team and Board of Governors with matters regarding e-Safety. All Governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice.

E-Safety and Staff / Skills Development

All staff will have a copy of the e-Safety policy and its application and importance explained.

All staff will receive regular updates of information and training on e-Safety issues through the ICT co-ordinator / team at meetings.
A monthly newsletter will go out to staff and parents detailing the most up to date information on E-Safety matters.

All staff are made and kept aware that all internet traffic is monitored and can be traced back to individual users.

All staff are made and kept aware of individual responsibilities relating to the safeguarding of pupils within the context of e-Safety so that they will know what to do in the event of misuse of technology by any member of the school community.

All staff will receive a copy of the e-Safety policy and Acceptable Use Agreement **(Appendix 3)** and sign an Acceptable Use Agreement which will include acceptable use of mobile devices such as mobile phones.

All staff are encouraged to incorporate e-Safety into their existing activities and promote awareness within their lessons.

New staff members will receive all of the above when / if necessary.

E-Safety and Pupils

E-safety will be discussed with all pupils at regular intervals throughout the school year (example, **Appendix 1**). Activities will include teacher led lessons and activities and lessons through outside agencies such as those for Safer Internet Day.

A pupil version of the Acceptable Use Agreement will be discussed with Year 3 pupils and will be signed by them and their parent / guardian at the start of the school year. **(Appendix 4)**

All pupils will follow a progressive Online Safety Curriculum aimed at insuring that they are equipped with the skills to keep them safe online, enabling them to become responsible digital citizens both now and in the future.

The e-Safety curriculum being followed is the collaborative work of the East Belfast Primary ICT Cluster Group, with guidance from the UK Council for Child Internet Safety.

E-Safety and Parents

The e-Safety policy will be made available to download on the school website; Parents will be encouraged to read this along with the other important school policies.

Parents of year 1 and year 2 pupils will be required to read the Acceptable Use Agreement and sign it on behalf of their child. **(Appendix 5)**

E-Safety will be promoted to Parents via the school website (example **Appendix 2**)and visits / talks from outside agencies such as the PSNI. Parents will be made aware of useful internet e-Safety sites such as CEOP and thinkuknow through links on the website.

A monthly newsletter will go out to parents detailing the most up to date information on E-Safety matters.

Teaching and Learning

Internet use:

Teachers will plan and provide opportunities within a range of curriculum areas to teach e-Safety.

Key e-Safety messages will be reinforced regularly throughout the school year. These will be tailored to the level our pupils are at, following the Scheme being used. (Appendix 1 and 2)

We as a school will liaise with other local schools to establish common approaches to e-Safety in the form of parent information workshops taken by local agencies or the PSNI.

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. Regardless, pupils’ use of the internet is closely supervised by an adult in all activities.

Use of the internet is part of planned activities. Pupils will not have access to any device for aimless internet surfing. Where a child has to use the internet as part of their lesson, specific instructions will be given and use 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 the Internet Safety Rules and encouraged to discuss how to cope 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.

<u>Online Safety During Periods of Remote Learning/Video calls</u>

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 video conferencing or platforms recommended by and available via C2K.

- Teachers and pupils need to be fully and appropriately dressed during the session.
- Pupils cannot participate from a bedroom.
- The teacher arranges the session and password/PIN and shares this only with pupils and their parents/guardians.
- Pupils must agree not to share the password/PIN with anyone else.
- Parents /Guardians will be informed of their child’s expected participation prior to first use. Pupils and parents/guardians will also be reminded of acceptable use at this point.
- Online sessions should be time limited for the benefit of both children and teachers.

If there is a breach to any of these procedures, the teacher should immediately terminate the session/remove those individuals and advise the Principal.

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

(Please see Blended Learning Policy for further information)

<u>Digital and Video Images of Pupils</u>

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 Dundela.

Regarding the use of digital and video images of Pupils, written permission will be 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.

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.

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, email, telephone and fax number. 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.
- Before content is published on the website for the general public to see it will have to be approved by a member of the website admin team.

Social Networking

Social networking sites are blocked by the C2K filtering system.

Staff who make personal use of social networking sites outside of school should not discuss any part of school life, pupils, staff or Parents in any way.

The use of social network spaces is inappropriate considering the age of our pupils. However, through e-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.

Mobile Technologies

Staff use of mobile phones, only when absolutely necessary, 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. Under no circumstances should personal devices be used to take photos of children.
Pupils are not permitted to bring mobile phones into school.

The use of portable media such as memory sticks will be monitored closely. In accordance to 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

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.

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

Staff are provided with individual login usernames and passwords are changed periodically. Staff should never share login details with anyone.

All pupils are provided with individual login usernames and passwords. Year 1 and year 2 pupils will use a simplified login. Year 3 pupils will use a standard C2K login with a password set initially by the teacher. They are encouraged to keep track of their own individual passwords further on in the school year.

Pupils are not allowed to deliberately access files on the school network which do not belong to them.

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.

School USB pen drives are password protected and is the responsibility of the individual staff member. Any loss of data or inappropriate access must be reported directly a member of the safe-guarding team / Principal.

Handling e-Safety Complaints

Complaints of internet misuse will be dealt with by the ICT and e-Safety coordinator Mrs. Yau who is our Designated Teacher of E Safety. She will inform a member of the safeguarding team / Principal if and when appropriate and will support the safeguarding team and parents when necessary.

Deliberate access to any inappropriate material by any user will be reported directly to the safe-guarding team/SLT/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

E Safety Rules for Children

Follow These SMART TIPS

S Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!

M Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

A Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

R Remember someone online may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

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

SMART Tips from: – Helping your parents be cool about the internet, produced by: Northern Area Child Protection Committees

Appendix 2

Under 5's checklist

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.html

Appendix 3

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. This Acceptable Use Agreement has been drawn up to protect all parties involved – pupils, staff and the school as a whole.

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 read and sign a copy of this Acceptable Internet Use Agreement and return it to the Principal / ICT co-ordinator.

- 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 activities that attack or corrupts other systems, is forbidden.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received.
- Use for personal financial gain, gambling, political purposes or advertising are forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As an e-mail can be forwarded or inadvertently sent to the wrong contact, the same professional levels of language and content should be applied as for letters and other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Social media should not be used in any way to directly discuss persons connected to the school or daily school life.
- Mobile phones should only be used discreetly during non-contact time.
- Staff take full responsibility for any school equipment taken and used off the school premises.

Signed: ________________________

Print Name: _________________________

Date: ________________________

Acceptable Use Agreement For Staff – Internet Streaming The new C2k Education Network introduces a revised system for internet filtering based on a Websense filtering solution. Websense assesses all websites based on their content and adds them to a category. 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, including those on the Internet Watch Foundation banned list will always remain blocked.

Note: The same C2k filtering applies across the C2k network, whether using a C2k core desktop computer or a personal iPad. This consistency is essential to ensure the safety and integrity of C2k's internet provision.

What's Different

Previously, primary schools had no school control over the internet sites available, and postprimary and special schools had access to a number of internet "amber groups" to which users could be added. The new system categorises all websites as either red (unavailable) or green (available). By default, all users are given access to a core set of green sites.

School choice:

In addition to the default sites, schools can choose to make users members of one or more internet-related security groups. These are:

- Internet Social Networking
- Internet Streaming Media
- Internet Advanced

Access to these groups is controlled by C2k Managers 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.

Dundels Infants' School and Nursery Unit Implications

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
- To in an appropriate manner and in accordance with the guidelines detailed in the school's E-Safety Policy and Child Protection Policy

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

Signed ___________________________________ Date ____________________

Appendix 4

Acceptable Use Agreement (Year 3)

Children should know that they are responsible for their use of the internet in school and that they do so in a safe and appropriate manner.

Pupils will discuss and agree to the following:

- On the school network I will only use my own login and password.
- I will keep my username and password private.
- I will not access other people's account / files without their permission.
- I will ask permission before entering any website, unless my teacher has already given permission.
- I will use the internet for research and school activities only.
- I must take care of and look after all of the school's ICT equipment which I am using.
- If I see anything that I am unhappy with or I do not like, I will tell my teacher immediately.
- I will not bring in memory sticks unless my teacher has given me permission to do so.
- I understand that if I break these rules I could be stopped from using the internet and my parents / guardians will be informed.

Signed by pupil: ________________________

Signed by parent / guardian: _________________________

Date: ________________________

Appendix 5

Acceptable Use Agreement (Year 1 and Year 2)

In any activity pupils' access to the internet will only be through demonstration or very close supervision.

Pupils are aware that they are responsible for their use of the internet in school and that they do so in a safe and appropriate manner.

Please read over the following and discuss with your child:

- On the school network they will only use their own login and password.
- They will not access other people's accounts without their permission.
- They will ask permission before entering any website, unless their teacher has already given them permission.
- They will use the internet for research and school activities only.
- They must take care of and look after all of the school's ICT equipment that they are using.
- If they see anything that they are unhappy with or do not like, they will tell their teacher immediately.
- They understand that if they break these rules they could be stopped from using the internet and parents / guardians will be informed.

Signed by parent / guardian: _________________________

Date: ________________________