

**Interview Record**

**Dromore Central Primary School**

**E-Safety Policy**

**D**

**E-Safety Policy**

**June 2023**

**Table of Contents**

1. General Statement Page 3
2. Rationale and Aims Page 3
3. Scope of Policy Page 4
4. Risk Assessment Page 4
5. Roles, Responsibilities and Training Page 5
6. Current Practice Page 9
7. Managing Incidents Page 12
8. Development, Monitoring and Review Page 14

E-Safety Policy

Ratified by Board of Governors (Date)\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Review Date: June 2023

1. **General Statement**

At Dromore Central Primary School we recognise the importance of ICT in the primary school curriculum. We believe it is a life skill that ranks alongside basic literacy and numeracy. We feel that it is our duty to provide staff and pupils in this school with the opportunity to develop the ICT capabilities and competences.

ICT comprises of a variety of systems that handle electronically retrievable information and as a school we recognise the crucial role that we have in raising awareness of the risks, highlighting the impact of behaviour when engaging with online technologies and educating children and young people about how to act appropriately and stay safe.

As Using Information and Communications Technology (UICT) is one of three cross curricular skills in the Northern Ireland Curriculum, with an emphasis on the use of ICT resources to enhance and enrich all areas of learning. We want our 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.

1. **Rationale**

*‘Schools have a responsibility to ensure that there is a reduced risk of pupils accessing harmful and inappropriate digital content. Schools should be energetic in teaching pupils how to act responsibly and keep themselves safe in the digital world and, as a result, pupils should have a clear understanding of online safety issues and be able to demonstrate what a positive digital footprint might look like for themselves.’* DENI Circular 2016/27.

It is the responsibility of staff and governors in the school/school-organised activities to safeguard and promote pupils’ welfare around digital technology.

**Aims**

Our E-Safety practice will:

* Address wider educational issues in order to help pupils (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* Cover not only internet technologies but also electronic communications via mobile phones, games consoles, wearable digital technologies and wireless technology.
* Incorporate agreements on the acceptable use of the Internet and school-based Digital Technology as well as Personal Mobile Technology.
* Allow pupils the opportunity to learn the positive benefits that come from learning, exploring and connecting with each other online.
* Promote appropriate online behaviour and give age relevant guidelines about how to stay safe.
* Safeguard and promote welfare around digital technology and provide a set of guiding principles for keeping pupils and the wider school community safe online.
* Prioritising online safety within the school’s preventative education curriculum and overall Safeguarding/Child Protection Policy.
* Provide a robust report channel for reporting online safety issues so that pupils and staff know who they can turn to if there is a problem.

1. **Scope of the Policy**

This policy applies to all members of the school community who have access to and are users of the school ICT systems, both inside and outside of school.

In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure E-Safety of all involved, apply sanctions as appropriate and review procedures.

In relation to E-Safety incidents that occur outside of school hours, the school will work with pupils and parents to keep all pupils safe and offer educative support where appropriate.

E-Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the school community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward.

Any issues that arise inside school, as a result of E-Safety incidents outside of the school, will be dealt with in accordance with School Policies.

1. **Risk Assessment**

The Safeguarding Board for Northern Ireland (SBNI) Report (January 2014) published its Report *‘An exploration of e-safety messages to young, people, parents and practitioners in Northern Ireland’*. It highlights the importance of protecting and educating children and young people as the use of technology and digital devices with online access continues to advance and impact on daily life.

The main areas of risk that comes with this extensive use of technology for the school can be defined and categorised as the Content, Contract and Conduct of activity.

* 1. Content

• Access to illegal, harmful or inappropriate images or other content.

• Access to unsuitable videos / internet games.

• An inability to evaluate the quality, accuracy and relevance of information on the Internet.

* 1. Contact

• Inappropriate communication / contact with others, including strangers.

• The risk of being subject to grooming by those whom they may make contract on the Internet.

• Cyber-bullying.

• Unauthorised access to/loss of/sharing of personal information.

* 1. Conduct

• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

• Plagiarism and copyright infringement.

• Illegal downloading of music or video files.

• The sharing / distribution of personal images without an individual’s consent or knowledge.

Many of these risks reflect situations in the offline world and it is essential that this E-Safety policy is used in conjunction with other School policies e.g. Positive Behaviour, Child Protection and Anti-Bullying. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

**Roles and Responsibilities**

|  |  |
| --- | --- |
| E-Safety Coordinators | Network Managers |
| Designated Child Protection Officers | Teaching and Support Staff |
| ICT Coordinators | Pupil members of the School Council |
| Principal and Senior Leadership Team | Parents/Carers |
| Governors | Community |

* **E-Safety Coordinators**

The E-Safety/ ICT Coordinators, Mrs Adams and Mrs J Snoddy, will take day to day responsibility for E-Safety issues and have a leading role in establishing and reviewing the Schools policies/documents. The E-Safety / ICT Coordinators will:

* Ensure that the members of staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place
* Provide training and advice for all members of staff .
* Liaise with C2K
* KS2 - Refer to the Google Safer Internet resources and guidance
* Liaise with the EA and DENI on E-Safety developments
* Receive reports of E-Safety incidents and create a log of incidents to inform future E-Safety developments
* Attend relevant meetings with Board of Governors
* Discuss current issues
* Review incident logs
* Monitor and report to the Senior Leadership Team any risks to staff of which the ICT coordinators are aware

**Designated Child Protection Officer / Designated Deputy Child Protection Officer**

The Child Protection Officer Mrs Y Mackay (and the deputy, Mrs H Bentley) will be trained in E-Safety issues 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

**ICT Coordinators will assist with**

* The production and review of the school E-Safety policy and related documents.
* Mapping and reviewing the e-safety curricular provision, ensuring relevance, breadth and progression.
* Monitoring incident logs from the pastoral team.
* Provide teaching materials and certificates for use on Safer Internet Day each February.
* Informing parents/carers and the pupils about the importance of E-Safety.

**The Principal and Senior Leadership Team**

The Principal has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day-to-day responsibility for E-Safety will be delegated to the ICT co-ordinators.

The Senior Leadership Team (SLT) will be kept informed about E-Safety incidents.

The Principal will deal with any serious E-Safety allegation being made against a member of staff. The Principal and SLT are responsible for ensuring that the staff receives suitable training to enable them to carry out their e-safety roles.

**Governors**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports.

The designated E-Safety Governor is Mrs. J. McBratney. She will;

• have regular meetings with the Principal

• regularly monitor E-Safety incidents logs

Training will be given to the Governors by:

• Attendance at training provided by relevant external agencies / staff in school

• Participation in school’s training / information sessions for staff or parents

**Network Managers**

The Network Managers, Mrs Adams and Mrs. J. Snoddy, will monitor that c2k E-Safety measures, as recommended by DENI, are working efficiently within the school. The Network Managers will also monitor that:

• c2k operates with robust filtering and security software.

• Monitoring reports of the use of C2k are available on request.

• The school infrastructure and individual workstations are protected by up-to-date virus software.

•The school meets required e-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 that its implementation is not the sole responsibility of any single person.

• They keep up to date with E-Safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

• Software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

• That the “administrator” passwords for the school ICT system, used by the Network Managers must also be available to the Principal and kept in a secure place

**Teaching and Support Staff**

The Teaching and Support Staff are responsible for ensuring that they have:

• Up-to-date awareness of e-safety matters and of the current school E-Safety policy and practices.

• Read, understood and signed the school’s Staff Acceptable Use Policy.

• Reported any suspected misuse or problem to the ICT Coordinators.

• Digital communications with students (email / Virtual Learning Environment (VLE) should be on a professional level only carried out using official school systems – either C2K, SeeSaw, Google Classroom or School email accounts. Emails should be sent in accordance with the School’s guidance.

• E-Safety issues are embedded in all aspects of the curriculum and other school activities.

• Staff understand and follow the school E-Safety Policy and Acceptable Use Policy.

• That students have a good understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act 1998.

• They monitor ICT activity in lessons, extracurricular and extended school activities.

• They are aware of e-safety issues related to the use of mobile phones, camera and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.

• Undertake all e-safety training as organised by the school

Professional Development for Teaching and Support Staff Training will be offered as follows:

• All new staff will receive e-safety training as part of their Induction Programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.

• A programme of e-safety training will be made available to staff if or when necessary.

• Staff will be made aware of the importance of the filtering system and be warned of the consequences of attempting to subvert the filtering system.

• This e-safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

**Pupil members of the Digital Leaders will assist the ICT Coordinators with**

• Potential issues regarding e-safety

• Present information during an assembly on ‘Safer Internet Day.’

• Pupils will only be expected to take part in staff committee meetings if deemed relevant.

**Pupils are responsible for ensuring that they have**

• A good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.

• Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• Know and understand school policies on the use of mobile phone, digital cameras, wearable digital technologies and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

• Pupils are introduced to email and taught about the safety and ‘etiquette’ of using e-mail both in school and at home.

• They understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s e-safety Policy covers their actions out of school, if related to their membership of the school.

E-Safety Education for Pupils E-Safety education for student will be provided in the following ways:

• Pupils will be taught in all relevant lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information and to respect Copyright when using material accessed on the Internet.

• Pupils will be helped to understand the need for acceptable use of ICT as well as being encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

• Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

**Parents / Carers Parents/Carers**

Parents / Carers Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and to support the E-Safety policy outlined by the School. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

• digital and video images taken at school events

• online communication with staff

• their children’s personal devices in the school

Parents/Carers have an essential role in the education of their children and in the monitoring and regulation of the children’s online behaviours. The school recognises that some parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The School will seek to provide information and awareness to parents and carers through:

• An E-Safety leaflet, distributed to all parents and then, subsequently, all new parents.

• Letters, newsletters, websites and Facebook posts.

• E-Safety Guidance will be delivered through key events.

**Community Users and Education for the Community**

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User Acceptable Use Policy before being provided with access to school systems.

The school will provide opportunities for members of the community to gain from the school’s E-Safety knowledge and experience through:

• The school website/Facebook

• Supporting community groups e.g. library staff/sports/voluntary groups to enhance their E-Safety provision

• Supporting other local schools and communicating with them to mutually enhance E-Safety provision.

1. **Current Practice**

Communication

• The official school email service may be regarded as safe and secure. Staff and pupils should therefore use the school email service, Seesaw or Google Classroom to communicate with others when in school, or on school systems (e.g. by remote access).

• Email communications with parents and/or pupils should be conducted through Seesaw, Google Classroom or the school email system ‘@c2ken.net’. Personal email addresses should not be used.

• Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

• Any digital communication between staff and pupils or parents/carers - email, VLE and official school social media accounts - must be professional in tone and content.

• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

• Further information is provided to staff during in service training, also see the ‘Email Policy’ for appropriate use.

**Social Networking**

At present, the school endeavours to deny access to social networking sites to pupils during school hours. Staff may use YouTube to disseminate information to pupils during school, if appropriate.

• The school will provide training in the appropriate use of social networking / for teaching and learning purposes.

• Training will include: acceptable use; social media risks; checking of settings; data protection; reporting issues; legal risks.

• Teachers should adhere to the social networking/communication guidance provided by the school.

• Teachers will receive advice in the appropriate use of social networking in their private life.

• Older students should be made aware of the appropriate and safe use of Social Networking.

• Teachers and pupils should report any incidents of cyber-bullying to the school.

• Further information is provided to staff during in service training, also see the ‘Social Media Policy’ for appropriate use.

**Pupils’ use of personal devices**

* Mobile Phones and personally-owned devices must be switched off, kept in school bags and not taken out or switched on in school.
* Wearable digital technologies that have the features to record / phone should not be brought onto school premises.

• If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

• Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.

• Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

• If a member of staff breaches the school policy then disciplinary action may be taken.

• Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. Where a staff member must use their own device, they should hide (by inputting 141) their own mobile number for confidentiality purposes.

• Further information is provided to staff/pupils/parents during in service training, also see the ‘Mobile Digital Devices Policy’ for appropriate use.

**CCTV**

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings, without permission, except where disclosed to the Police as part of a criminal investigation.

* Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with taking digital images and sharing on the Internet.

When using digital images, staff informs and educates pupils about the risks associated with taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. Social Networking websites.

The school gains parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those image/s.

We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Pupils must not take, use, share, publish or distribute images of others without their permission.

The use of digital / video images plays an important part in learning activities.

The school will comply with the Data Protection Act by requesting parents’ permission when their child starts school in Year 1. Permission will last until the student leaves school, unless a parent/carer provides a written withdrawal of taking images of members of the school.

**Teaching and Support Staff**

Password Security Password security is essential for staff, particularly as they are able to access and use student data.

* Staff are expected to have secure passwords which are not shared with anyone.
* Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.
* Individual staff users must also make sure that workstations/iPads are not left unattended and are locked.
* Further information is provided to staff during INSET training.

The principal Mrs L Allen and the vice principal Mrs H Bentley will approve the staff access to modules in SIMS for the purposes of assessment, SEN, contact information and attendance.

Teachers will deliver an age related online safety curriculum to enable pupils to become safe and responsible users of technology.

Teachers will fill in and log any incidents of online safety issues within the school intranet system STAFF area in a folder entitled ‘Online Risk Register’.

**Students: Password Security**

• Students are expected to keep their passwords secret and not to share with others, particularly their friends.

• Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

1. **Managing Incidents**

**Cyber-bullying**

Cyber Bullying can take many different forms and guises including:

• Email – nasty or abusive emails which may include viruses or inappropriate content.

• Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.

• Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user’s profile.

• Online Gaming – abuse or harassment of someone using online multi-player gaming sites.

• Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves, and these are subsequently transmitted to other people. Abusing Personal Information – may involve the posting of photos, personal information, fake comments, and blogs, or pretending to be someone online without that person’s permission.

Incidents of cyber–bullying will be dealt with in accordance with the School Anti-Bullying Policy as well as the Safe-Guarding and Child Protection Policies.

**Social Media**

The school uses our school Facebook page as a means of communicating directly with parents/carers and the wider community. Our new school website has a direct notice and email facility that must be signed up to by parents/carers wishing to have a web-based interaction with the school.

**The Data Protection Act**

The school has a Data Protection Policy and staff are regularly reminded of their responsibilities. In particular, staff must ensure that they at all times:

• Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

• Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media, it is advisable that:

• the device is password protected

• it has approved virus and malware checking software

• the data is securely deleted from the device, in line with school policy, once it has been transferred or its use is complete

**Filtering**

Technical Framework Filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. This is provided as part of the core 2k EnNI service in all schools and ensures that this provision removes the need for any school to continue to have a second line/network in place as stipulated in the DE letter to schools dated 18 September 2014.

The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. The responsibility for the management of the school’s filtering policy is held by The Principal and coordinators in review of the DE Circular 2015/21 about School obligations to manage data. They manage the school filtering by:

• Monitoring reports of the use of C2k which are available on request

• Keep records and logs of changes and of breaches of the filtering systems.

• These changes and breaches should be reported to the ICT Coordinators.

Staff and pupils have a responsibility to:

• Report immediately to ICT Coordinator/s any infringements of the school’s filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials. The Senior Leadership team will ensure that the additional Wi-Fi systems installed within the school do not undermine or adversely impact on the overall effectiveness of the school’s child protection and safeguarding polices.

Auditing and reporting:

Logs of filtering change controls and of filtering incidents will be made available to:

• ICT Coordinators

• Board of Governors

• External Filtering provider / Police on request

**Actions and Sanctions**

Sanctions for the misuse of technology are outlined in the Acceptable Use Policy: Further to this, should technology or online platforms be used as a means by which to bully another, the sanctions detailed in the Anti-Bullying Policy will be implemented.

In case of Internet abuse or where a child is at risk the school’s child protection procedures should be implemented.

1. **Development, Monitoring and Review**

**Schedule for Developing, Monitoring and Reviewing Policy Approval by the Board of Governors:**

The implementation of this E-Safety policy will be monitored by:

* The ICT Coordinators

The Board of Governors will receive reports on E-Safety including anonymous details of E-Safety incidents. Should serious E-Safety incidents take place, the following external persons or agencies should be informed:

* PSNI
* Chair of Board of Governors
* EA

**Monitoring and Reviewing**

* Annually and/or if required following a breach of safety.