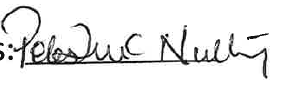
Sion Mills Primary School and Nursery Unit

E-Safety Policy

Updated by: K. Cunningham (ICT Coordinator)

Signed by Principal: 

Date ratified by Board of Governors: 20/09/2022

Signed by Chair of Governors: 

Next review date: September 2024



# Online Safety Policy

The school Online Safety Policy:

* sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
* allocates responsibilities for the delivery of the policy.
* is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
* establishes guidance for staff in how they can use digital technologies responsibly, protecting themselves and the school and how they can use this understanding to help safeguard learners in the digital world.
* describes how the school will help prepare learners to be safe and responsible users of online technologies.
* establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
* is supplemented by a series of related acceptable use agreements.
* is made available to staff at induction and through normal communication channels.
* is published on the school website.

# Introduction

# This policy is based on and complies with DENI circular 2016/27 on *Online Safety*. (Appendix 1) It has been updated in relation to the *Keeping children and young people safe: an online Safety Strategy for Northern Ireland 2020-2025.* (Appendix 2)

**This policy applies to all members of the schoolcommunity (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).**

Sion Mills Primary School believes that the internet and other digital technologies are very powerful resources which can potentially transform teaching and learning when used effectively and appropriately. The internet is an essential element of modern day living for education, business and social interaction. Article 17 of the UNICEF Charter of rights states that:

***“Children have the right to get information from the Internet, radio, television, newspapers, books and other sources. Adults should make sure the information they are getting is not harmful. Governments should encourage the media to share information from lots of different sources, in languages that all children can understand.”****[[1]](#footnote-1)*

Our 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. Internet use is part of the statutory UICT curriculum and a necessary tool for staff and pupils.

The above circular 2016/27 states that:

***Online safety, in all cases, in schools and elsewhere, remains a paramount concern. Schools play a crucial role in raising awareness of the risks, highlighting the impact of behaviour when engaging with online technologies and education children and young people about how to act appropriately and stay safe.****[[2]](#footnote-2)*

This document sets out the policy and practices for the safe, healthy, acceptable and effective use of the internet in Sion Mills Primary School. The policy has been drawn up by the staff of the school under the leadership of Mrs K. Cunningham, ICT coordinator. It has been approved by the Board of Governors and is available to parents via the school website. <https://www.sionmillsps.com/> A hard copy can be requested. The policy and its implementation will be reviewed biannually. The school will monitor (Appendix 5) the impact of the policy using:

* logs of reported incidents
* monitoring logs of internet activity (including sites visited)
* internal monitoring data for network activity
* surveys/questionnaires of: learners, parents and carers and staff.

1. **C2k**

Classroom 2000 (C2k) is the project responsible for the provision of information and communications technology (ICT) managed services to schools in Northern Ireland. It provides a safety service which should ensure educational use of resources is safe and secure, while protecting users and systems from abuse.

Some of the safety services include:

* providing all users with a unique name and password.
* Tracking and recording all online activity using the unique names and passwords.
* Scanning all C2k email and attachments for inappropriate content and viruses.
* Filters access to websites.
* Providing appropriate curriculum software.

Should the school decide to provide an alternative online service then we will ensure that effective firewalls, filtering and software monitoring mechanisms are provided.

1. **Code of Safe Practice**

When using the internet, email systems, online learning platforms and digital technologies all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. (A list can be found in Appendix 3)

The Code of Safe Practice for Sion Mills PS and Nursery Unit makes it explicit to all users (staff and pupils) what is safe and acceptable and what is not. The scope of the code covers fixed and mobile internet; school PCs, laptops, chrome books, iPads, Surface Pros and digital video equipment. It should be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones) are subject to the same requirements as technology provided by the school.

**Code of Safe Practice for Pupils**

A parental/carer letter accompanied by a Parental Consent form and the Code of Safe Practice for Pupils is sent out annually. (Appendix 4a and 4b) This consent must be obtained before pupils can access the internet.

In addition, the following key measures have been adopted by Sion Mills PS and Nursery Unit to ensure our pupils do not access any inappropriate material.

* The school’s Code of Safe Practice is made explicit to all pupils and is displayed prominently.
* It is reviewed each school year.
* Pupils who use the internet will work 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 the age group.
* Pupils in all key stages, at an appropriate level, are educated in the safe and effective use of the internet, through a number of selected websites, schemes of work (<https://projectevolve.co.uk/>) and safer Internet day.

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school or C2k can accept liability under such circumstances. Staff and pupils will report any unsuitable websites and their URL to the ICT Coordinator who will in turn inform C2k.

The use of mobile phones by pupils is not permitted on the school premises during school hours. (See Mobile Phone Policy)

**Sanctions**

Incidents of technology misuse which arise will be dealt with in accordance with the school’s Positive Behaviour policy. Minor incidents will be dealt with by the ICT coordinator and the principal and may result in a temporary or permanent ban on Internet use. Records will be kept by the coordinator (Appendix 5). Incidents involving child protection issues will be dealt with in accordance with school’s Child Protection policy.

# **Code of Safe Practice for Staff**

11

The following Code of Safe Practice has been agreed with staff. Staff are required to sign an E-Safety Staff Acceptable Use agreement. (Appendix 4c)

* All staff will be given the school E-safety Policy and its application and importance explained.
* All staff will receive regular information and training on E-safety issues.
* Staff should be aware that internet traffic (including websites visited, emails sent and received) can be monitored and traced to the individual user. Discretion and professional conduct is essential. These things are tracked by C2k system.
* All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
* All staff sign the E-safety Staff Acceptable Use Agreement annually. They are notified of any changes.
* All teachers must incorporate E-safety into their lessons based on NI curriculum.
* All staff are asked to use their C2k e-mail system and are strongly advised not to use their home e-mail account for school business.
* Pupils accessing the internet should be supervised by an adult at all times.
* Staff will make pupils aware of the rules for safe and effective use of internet. These should be displayed in classrooms and areas where ICT equipment is used.
* All pupils must have written permission from legal guardians to use the internet.
* Deliberate/accidental access to inappropriate materials or any other breaches of school code of safe practice should be reported immediately to the principal/coordinator.
* In the interests of system security staff passwords should only be shared with C2k manager.
* Staff should be aware of copyright and intellectual property rights and should be careful not to download or use any material which are in breach of these.
* Photographs of pupils should, where possible, be taken with only a school device and images stored on a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work. School systems may not be used for unauthorised commercial transactions (See Photographic Permissions policy)

1. **Internet Safety Awareness**

In Sion Mills Primary and Nursery, we believe that alongside having a written E-safety policy and Code of Safe Practice, it is essential to educate all users in the safe and effective use of the internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience. This education is important for staff and parents as it is for pupils. The Safer Schools NI app has been introduced to our school community to aid both information and education for all stakeholders.

**PUPILS**

*Safety rules and acceptable use are prominently displayed in classrooms and ICT room.*

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and may be provided in the following ways;

* a planned online safety curriculum across all year groups and a range of topic areas and should be regularly revisited. *(Project Evolve, UK Safer Internet Centre, Childnet Get Smart, ThinkUKnow, Google Internet Legends)*
* key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
* Pupils will be made aware that the C2k network and internet use will be monitored
* it incorporates/makes use of relevant national initiatives and opportunities e.g. [Safer Internet Day](https://hwb.gov.wales/zones/keeping-safe-online/safer-internet-day/) and [Anti-bullying week](https://www.anti-bullyingalliance.org.uk/anti-bullying-week)
* the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language. Learners considered to be at increased risk online (e.g. children in care, SEND learners, learners experiencing loss or trauma or mental health issues) are provided with targeted or differentiated online safety education
* learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
* learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
* learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
* staff should act as good role models in their use of digital technologies the internet and mobile devices
* in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
* where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
* the online safety education programme will be regularly audited and evaluated to ensure the quality of learning and outcomes.

**STAFF**

* The coordinator and the ICT team keep updated and informed on issues relating to internet safety. All staff are in turn made aware of policy and strategy on ICT use in teaching and learning and updated about relevant changes.
* All staff informed that the network and internet use can be monitored and traced to individual user.
* Staff will use child friendly search engine when accessing web with pupils (<https://www.kiddle.co/> or <https://swiggle.org.uk/> )
* Staff are aware of the Chile Exploitation and Online Protection Centre (CEOP) website for advice/training and lessons.

**PARENTS**

* E-safety and Code of Safe Practice available online and sent to each family annually.
* Permission requested for internet use in school.
* Internet safety leaflets/promoting e-safety at home. (Appendix 6)
* Links on school website.
* Relevant e-safety information communicated through newsletters, School Facebook page and/or Seesaw app.

**Community Use of School ICT Resources**

The school’s ICT resources may be used a community resource under the Extended School’s programme. Users (not pupils attending Sion Mills PS) are issued with separate usernames and passwords by C2k. They must also agree to the school’s Use of the Internet Policy before participating and only access pre-selected and appropriate websites under the guidance of a tutor.

1. **Health and Safety**

In Sion Mills PS and Nursery Unit we have attempted, in so far as possible, to ensure a safe, working environment for pupils and teachers using ICT resources, both in classrooms and in the computer room, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when interactive whiteboards are being used. Guidance is also issued to pupils in relation to the safe use of computers, IPads and interactive whiteboards. Such guidance includes advice concerning correct posture, screen position and not looking directly at any projector. We are mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

**Use of mobile phones**

See school’s Acceptable use of Mobile Phones Policy.

**Wireless network**

The health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposers below guidance levels and therefore no reason why schools and others should not use Wi-Fi equipment. Further information on this can be found at the [Health Protection Website.](https://www.publichealth.hscni.net/)

1. **School Online Presence**

**Website**

This is used to celebrate pupils’ work, promote the school and provide information. Our website reflects the school’s ethos that information is accurate and well-presented and that personal security is not compromised. As the website can be accessed by anyone on the internet, the school has to be very careful to safeguard the interests of it pupils and staff. The following rules apply:

* Point of contact on the website will be the school address, school email and telephone number. Staff or pupils’ information will not be published.
* Website photographs will be selected carefully. Written permission from guardians will be obtained to allow photographs to be published. Pupils’ full names will not be used.
* The Vice-principal and a 2 other staff members will take overall editorial responsibility and ensure that content is accurate and appropriate.
* Website will comply with school’s guidelines for publications.
* Copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

**Facebook Page**

This is used to celebrate pupils’ work, promote school events and achievements and provide information. The social media account is maintained by a Board of Governors Rep and all permanent teaching staff have access to make posts. In parallel with the website the content should be accurate, well-presented and personal security should not be compromised. The same rules for website apply to the Facebook page.

1. **Social Software**

This is a generic term for community networks, chatrooms, instant messenger systems, online journals, social networks and blogs. Social environments enable any community to share resources and ideas amongst users. The majority of activity in this area usually causes no concern. C2k filters out social networking sites and attempts to circumvent their filters leaving it relatively safe in the school environment. Concerns in relation to inappropriate activities would tend to come from outside the school environment. We regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through out internet safety education for all pupils.

Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school’s Positive behaviour policy, Child-protection policy and Anti-bullying policy procedures. Pupils are aware that any misuse of mobile phone/website/email should be reported to a member of staff immediately.

The school will take very seriously any behaviour by a pupil or parent online that could bring the school’s name into disrepute. This will include any derogatory information or postings about staff or pupils. The school will not hesitate to involve outside agencies such as PSNI or to seek legal advice on such matters.

**Appendices**

1. [DENI Circular 2016/27 **Online Safety**](https://www.eani.org.uk/publications/safeguarding-and-child-protection/circular-201627-online-safety)
2. [Keeping Children and Young People Safe: An Online Strategy for Northern Ireland](https://www.health-ni.gov.uk/publications/online-safety-strategy-and-action-plan)
3. Legislation

4a. Letter to parents and consent for internet use.

4b. E-safety pupil contract

4c. E-safety staff contract

1. Monitoring forms
2. Promoting e-safety in the home. <https://ictinschools.org/e-safety/online-safety-at-home/>

# **Appendix 3**

# **Legislation**

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the event of an online safety issue or situation.

### *Computer Misuse Act 1990*

This Act makes it an offence to:

* erase or amend data or programs without authority;
* obtain unauthorised access to a computer;
* “eavesdrop” on a computer;
* make unauthorised use of computer time or facilities;
* maliciously corrupt or erase data or programs;
* deny access to authorised users.

Schools may wish to view the National Crime Agency (NCA) website which includes information about “[Cyber Choices: Helping you choose the right and legal path](https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices)”. The [TARIAN Regional Cyber Crime Unit (RCCU)](https://www.tarianrocu.org.uk/cyber-prevent/) now has dedicated ‘Cyber Prevent’ officers whose role is to prevent young people from committing cybercrime and/or re-offending. [Supportive resources are available on Hwb](https://hwb.gov.wales/search?query=tarian&strict=true) and there is a useful [summary of the Computer Misuse Act on the NCA site](https://nationalcrimeagency.gov.uk/who-we-are/publications/75-guide-to-the-computer-misuse-act/file).

### *Data Protection Act 1998*

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

* fairly and lawfully processed
* processed for limited purposes
* adequate, relevant and not excessive
* accurate
* not kept longer than necessary
* processed in accordance with the data subject’s rights
* secure
* not transferred to other countries without adequate protection.

### *The Data Protection Act 2018:*

#### Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

* facilitate the secure transfer of information within the European Union
* prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business
* give the public confidence about how businesses can use their personal information
* provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it
* give data subjects greater control over how data controllers handle their data
* place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they’re securely handling data
* require firms to keep people’s personal data safe and secure. Data controllers must ensure that it is not misused
* require the data user or holder to register with the Information Commissioner’s Office (ICO).

#### All data subjects have the right to:

* receive clear information about what you will use their data for
* access their own personal information
* request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
* request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan
* prevent or query about the automated processing of their personal data.

### *Freedom of Information Act 2000*

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

### *Communications Act 2003*

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

### *Malicious Communications Act 1988*

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

### *Regulation of Investigatory Powers Act 2000*

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

* establish the facts
* ascertain compliance with regulatory or self-regulatory practices or procedures
* demonstrate standards, which are or ought to be achieved by persons using the system
* investigate or detect unauthorised use of the communications system
* prevent or detect crime or in the interests of national security
* ensure the effective operation of the system
* monitoring but not recording is also permissible in order to:
  + ascertain whether the communication is business or personal
  + protect or support help line staff
* the school reserves the right to monitor its systems and communications in line with its rights under this act.

### *Trade Marks Act 1994*

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

### *Copyright, Designs and Patents Act 1988*

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

### *Telecommunications Act 1984*

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

### *Criminal Justice & Public Order Act 1994*

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

* use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
* display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

### *Racial and Religious Hatred Act 2006*

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### *Protection from Harassment Act 1997*

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

### *Protection of Children Act 1978*

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

### *Sexual Offences Act 2003*

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

### *Public Order Act 1986*

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

### *Obscene Publications Act 1959 and 1964*

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

### *Human Rights Act 1998*

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

* the right to a fair trial
* the right to respect for private and family life, home and correspondence
* freedom of thought, conscience and religion
* freedom of expression
* freedom of assembly
* prohibition of discrimination
* the right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

### The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

### *Serious Crime Act 2015*

This Act introduced a new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE).

### *Criminal Justice and Courts Act 2015*

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison. For further guidance or support please contact the [Revenge Porn Helpline](https://revengepornhelpline.org.uk/)

Appendix 4a

**Sion Mills Primary School,**

**The Park, Sion Mills,**

**Strabane, Co. Tyrone.**

**BT82 9HP**

**Phone No: (028) 816 58249**

**Fax No: (028) 816 59645**

**E-mail:** [**oncnelis240@sionmills.strabane.ni.sch.uk**](mailto:oncnelis240@sionmills.strabane.ni.sch.uk)

**Dear Parent/Guardian,**

**Internet Access for Pupils**

As part of our school’s UICT programme, we offer pupils supervised access to a filtered internet service, provided by C2k. This allows pupils access to a large array of online resources which we believe can greatly enhance their learning experiences. Various projects have proven the educational benefits of internet access, which will enable pupils to explore thousands of libraries, databases and websites. They will also be able to exchange messages with other learners and teachers throughout the world. Although internet use is filtered and supervised in our school, families will wish to be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people. We believe that the benefits to pupils from access to the internet in the form of information resources and opportunities for collaboration, exceed any disadvantages.

Access to and the use of the internet requires responsibility on the part of the user and the school. We in school, take active steps to promote the safe use of the internet. I am writing to obtain parental permission for your child to use the internet. Both they and you must sign and return the form enclosed as evidence of your approval and acceptance of the e-safety agreement.

However, as with any other area, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. The school therefore supports and respects each family’s right to decide whether or not to agree to internet access. During school, teachers will guide pupils towards appropriate material. At home, families bear the same responsibility for guidance as they exercise with TV, mobile phones, films and games.

An information leaflet ‘Promoting e-safety in the home’ is included. You can also access our e-safety policy from the school website. Any questions please contact the school to speak to the ICT coordinator.

Yours sincerely

O McNelis

Principal



|  |  |  |
| --- | --- | --- |
| **This consent form is valid for the academic year 2022 – 2023** | YES | NO |
| I give permission for photographs, voice recordings, videos of my child and his/her work to be taken and displayed within the school. |  |  |
| I give permission for photographs of my child to be used in the printed school Newsletter. I understand that this Newsletter is posted in pdf format on the school website. |  |  |
| I give permission for photographs, voice recordings or videos of my child and his/her work to be used on the School's website and our school-managed social media portals eg Facebook. |  |  |
| My child may be named in the associated images, captions or articles on the website or school-managed social media portals. |  |  |
| My child’s image, voice or work may be used in school promotional materials, for example: prospectus, annual BOG Report, other publications that we produce for promotional purposes. |  |  |
| I give permission for visiting media organisations (eg local newspapers) to take photographs or video footage of my child and use them in local or national publications, on websites and on radio or television programmes.  (\*In these instances full names are sometimes used). |  |  |

**Parents/legal guardians of pupils under the age of 13 or pupils should complete this form on behalf of the pupil.**

|  |
| --- |
| **PERMISSION SLIP FOR USE OF INTERNET** |
| We have discussed the “Rules for Responsible Computer, Portable Devices and Internet Use” or “Pupil e-safety agreement”. As the parent or legal guardian of the pupil signing below, I grant permission for my child to use the Internet in school. I understand that Internet access is intended for educational purposes and we must use it responsibly. I also understand that some material on the Internet may be objectionable and I accept responsibility for promoting standards for my son or daughter to follow. I understand that every reasonable precaution has been taken by school to provide for on-line safety.  **Please circle -** I do\* / do not\* give permission for my child to access the C2K Network and use the Internet  Parent/Guardian signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  I understand the School rules for the use of School computers and the Internet and I agree to follow them.  Pupil’s signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

*If you have any queries regarding the above statements/permission, please contact the class teacher*.

Appendix 4b

**Sion Mills Primary School – e-safety Pupil Contract**

**Rules for responsible computer, portable devices and internet use. (P5-7)**

*Sion mills PS has C2k network installed computers or laptops in each classroom and in a central computer room. Pupils have access to Chrome books and IPads also. All of these devices have internet access to help our learning. These rules will keep everyone safe and help us to fair to others.*

* I will always make sure a member of staff is present when I log on.
* I understand I must take care of school ICT equipment I use.
* I will keep my username and password private and not tell anyone else.
* I will not attempt to log on as another person by using their name and password.
* I will not access other people’s work, folders or files.
* I will use ICT equipment for educational purposes.
* I will follow the teacher’s instructions for using the internet.
* I will ask permission before using any website unless approved by my teacher.
* I will not bring memory pens or other external storage devices unless given permission.
* I will email my teacher or others when given permission and use only my school email address.
* The messages I send will be polite and sensible.
* I will not share personal information about myself or others when online.
* If I see something that makes me feel uncomfortable I will tell an adult immediately.
* I understand that my use of ICT can be checked and that a parent/guardian will be contacted if staff are concerned about my use of the internet.
* I understand that if I choose to break these rules I may no longer be allowed to use either school ICT equipment or the internet for a time.

**Sion Mills Primary School – Pupil e-safety Agreement (P1-P4)**

*Keeping me safe at home and at school.*

* I will ask a teacher or suitable adult if I want to use the computers/tablets.
* I will only use activities that a teacher or suitable adult has told or allowed me to use.
* I will take care of computers/tablets and other equipment.
* I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
* I will tell a teacher or suitable adult if I see something that upsets me on the screen.
* I know that if I break the rules I might not be allowed to use a computer/tablet.



Appendix 4c

**Sion Mills Primary School and Nursery Unit- e-safety Staff Contract**

*ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere to its contents. Any concerns or clarification should be discussed with the ICT/e-safety coordinator or the principal.*

* I will only use the school’s email/internet and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the principal or Board of Governors.
* I will comply with the C2k system security and not disclose to anyone any log-in or password details provided to me by the school or other related authorities.
* I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
* I will not give out my own personal details, such as phone number, email address (not C2k) to pupils or parents.
* I will only use the approved, C2k, secure e-mail system for any school business.
* I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.
* I will not install and hardware/software or purchase anything through the school iTunes account without the permission from a C2k manager.
* I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
* Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy.
* I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available on request, to C2k managers or principal.
* I will log out when finished using a computer or laptop.
* I will request copyright and intellectual property rights.
* I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
* I will support and promote the school’s e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

**User Signature**

I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school.

Signature…………………………………………………………………………… Date………………………………………………………….

Full Name (Printed) …………………………………………………………………………………. Job Title ……………………………………………………….

Appendix 5

**E-Safety Incident Log**

Details of ALL e-Safety incidents should be recorded by the e-Safety Coordinator. This incident log will be monitored regularly by a designated senior manager. Any incidents involving Cyberbullying should be recorded on the ‘Bullying Incident Log’ if one is maintained by your organisation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Date & Time*** | ***Name of child & staff member*** | ***Room no. & Device no.*** | ***Details of Incident & Evidence*** | ***Actions and Reasons*** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| User actions 18 | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | child sexual abuse images – the making, production or distribution of indecent images of children, contrary to The Protection of Children Act 1978  N.B. Schools should refer to [guidance about dealing with nudes and semi-nudes being shared](https://hwb.gov.wales/news/articles/97931dfd-3fe4-4514-967a-7038f421726a). |  |  |  |  | X |
| grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003 |  |  |  |  | X |
| possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008 |  |  |  |  | X |
| criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 |  |  |  |  | X |
| pornography |  |  |  | X |  |
| promotion of any kind of discrimination |  |  |  | X |  |
| threatening behaviour, including promotion of physical violence or mental harm |  |  |  | X |  |
| promotion of extremism or terrorism |  |  |  | X |  |
| any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute |  |  |  | X |  |
| Activities that might be classed as cyber-crime under the Computer Misuse Act (1990):   * Using another individual’s username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) * Gaining unauthorised access to school networks, data and files, through the use of computers/devices * Creating or propagating computer viruses or other harmful files * Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) * Disable/Impair/Disrupt network functionality through the use of computers/devices * Using penetration testing equipment (without relevant permission)   N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information [here](https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved) | |  |  |  |  | X |
| Using school systems to run a private business | |  |  |  | X |  |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | |  |  |  | X |  |
| Infringing copyright | |  |  |  | X |  |
| Revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords) | |  |  |  | X |  |
| Creating or propagating computer viruses or other harmful files | |  |  |  | X |  |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | |  |  |  | X |  |
| Online gaming (educational) | |  |  |  |  |  |
| Online gaming (non educational) | |  |  |  |  |  |
| Online gambling | |  |  |  |  |  |
| Online shopping/commerce | |  |  |  |  |  |
| File sharing | |  |  |  |  |  |
| Use of social media | |  |  |  |  |  |
| Use of messaging apps | |  |  |  |  |  |
| Use of video broadcasting, e.g. YouTube  19 | |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Staff and other adults** | | |
| Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission |
| Mobile phones may be brought to school |  |  |  |  |  |  |  |
| Use of mobile phones in lessons |  |  |  |  |  |  |  |
| Use of mobile phones in social time |  |  |  |  |  |  |  |
| Taking photos on mobile phones/cameras |  |  |  |  |  |  |  |
| Use of other mobile devices, e.g. tablets, gaming devices |  |  |  |  |  |  |  |
| Use of personal e-mail addresses in school, or on school network |  |  |  |  |  |  |  |
| Use of school e-mail for personal e-mails |  |  |  |  |  |  |  |
| Use of messaging apps |  |  |  |  |  |  |  |
| Use of social media |  |  |  |  |  |  |  |
| Use of blogs |  |  |  |  |  |  |  |

## Learner actions

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Incidents** | Refer to class teacher/tutor | Refer to Head of Department/Head of Year/other | Refer to Headteacher/Principal | Refer to Police | Refer to technical support staff for action re filtering/security etc. | Inform parents/carers | Removal of network/internet access rights | Issue a warning | Further sanction, e.g. detention/exclusion |
| Deliberately accessing or trying to access material that could be considered illegal (see list [in earlier section](#_User_actions) on unsuitable/inappropriate activities). |  | X | X | X |  |  |  |  |  |
| Unauthorised use of non-educational sites during lessons. |  |  |  |  |  |  |  |  |  |
| Unauthorised use of mobile phone/digital camera/other mobile device. |  |  |  |  |  |  |  |  |  |
| Unauthorised use of social media/messaging apps/personal e-mail. |  |  |  |  |  |  |  |  |  |
| Unauthorised downloading or uploading of files. |  |  |  |  |  |  |  |  |  |
| Allowing others to access school network by sharing username and passwords. |  |  |  |  |  |  |  |  |  |
| Attempting to access or accessing the school network, using another learners’ account. |  |  |  |  |  |  |  |  |  |
| Attempting to access or accessing the school network, using the account of a member of staff. |  |  |  |  |  |  |  |  |  |
| Corrupting or destroying the data of other users. |  |  |  |  |  |  |  |  |  |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature. |  |  |  |  |  |  |  |  |  |
| Continued infringements of the above, following previous warnings or sanctions. |  |  |  |  |  |  |  |  |  |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. |  |  |  |  |  |  |  |  |  |
| Using proxy sites or other means to subvert the school’s filtering system. |  |  |  |  |  |  |  |  |  |
| Accidentally accessing offensive or pornographic material and failing to report the incident. |  |  |  |  |  |  |  |  |  |
| Deliberately accessing or trying to access offensive or pornographic material. |  |  |  |  |  |  |  |  |  |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.  21 |  |  |  |  |  |  |  |  |  |

## Staff Actions

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Incidents** | Refer to line manager | Refer to Headteacher/ Principal | Refer to local authority/HR | Refer to Police | Refer to Technical Support Staff for action re filtering, etc. | Issue a warning | Suspension | Disciplinary action |
| **Deliberately accessing or trying to access material that could be considered illegal (see list** [**in earlier section**](#_User_actions) **on unsuitable/inappropriate activities)** |  | X | X | X |  |  |  |  |
| Inappropriate personal use of the internet/social media/personal e-mail |  |  |  |  |  |  |  |  |
| Unauthorised downloading or uploading of files. |  |  |  |  |  |  |  |  |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account. |  |  |  |  |  |  |  |  |
| Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner |  |  |  |  |  |  |  |  |
| Deliberate actions to breach data protection or network security rules. |  |  |  |  |  |  |  |  |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software |  |  |  |  |  |  |  |  |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature. |  |  |  |  |  |  |  |  |
| Using personal e-mail/social networking/messaging to carrying out digital communications with learners and parents/carers |  |  |  |  |  |  |  |  |
| Actions which could compromise the staff member’s professional standing |  |  |  |  |  |  |  |  |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. |  |  |  |  |  |  |  |  |
| Using proxy sites or other means to subvert the school’s filtering system. |  |  |  |  |  |  |  |  |
| Accidentally accessing offensive or pornographic material and failing to report the incident. |  |  |  |  |  |  |  |  |
| Deliberately accessing or trying to access offensive or pornographic material |  |  |  |  |  |  |  |  |
| Breaching copyright or licensing regulations. |  |  |  |  |  |  |  |  |
| Continued infringements of the above, following previous warnings or sanctions. |  |  |  |  |  |  |  |  |

22

# A3 Learner Acceptable Use Policy Agreement Template – for younger pupils

### This is how we stay safe when we use computers:

### Signed (child):

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent/carer should be sufficient)

### Signed (parent):

Primary schools using this acceptable use agreement for younger children may also wish to use (or adapt for use) the parent/carer acceptable use agreement (the template can be found later in these templates) as this provides additional permission forms (including the digital and video images permission form).

# A4 Parent/Carer Acceptable Use Agreement Template and permission forms

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### This acceptable use policy is intended to ensure:

* that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
* that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the learners in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work. (Schools will need to decide whether or not they wish parents to sign the acceptable use agreement on behalf of their child)

### Permission Form

### Parent/Carers Name: Name(s) of Learners

As the parent/carer of the above learners, I give permission for my child to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

*I know that my child has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.*

Or: (Foundation)

*I understand that the school has discussed the acceptable use agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of the school.*

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child’s activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

|  |
| --- |
| This form (electronic or printed) |
| Who will have access to this form. |
| Where this form will be stored. |
| How long this form will be stored for. |
| How this form will be destroyed. |

### Signed:

### Date:

When complete, ensure the information on this form is recorded in the school database.

Paper copies should be securely destroyed.

When complete, this page should be stored in a secure location for the duration of:

*insert period*

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

# A9 Record of reviewing devices/internet sites

# **(responding to incidents of misuse)**

School:

Date:

Reason for investigation:

### Details of first reviewing person

Name:

Position:

Signature:

### Details of second reviewing person

Name:

Position:

Signature:

### Name and location of device used for review (for web sites)

|  |  |
| --- | --- |
| Web site(s) address/device | Reason for concern |
|  |  |
|  |  |
|  |  |

### Conclusion and action proposed or taken

|  |  |
| --- | --- |
|  |  |
|  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A10 Reporting Log School: | | | | | | | | | |
| Date | Time | Incident | | Action Taken | | | Incident Reported By | | Signature |
| What? | | By Whom? |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
| B1 Training Needs Audit Log School: | | | | | | | | | |
| Relevant training in the last 12 months | | | Identified Training Need | | To be met by | | | Cost | Review Date |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |

1. <https://www.unicef.org/media/56661/file> Visited 25/8/2022 [↑](#footnote-ref-1)
2. <https://www.education-ni.gov.uk/publications/circular-201627-online-safety> Visited 25/8/2022 [↑](#footnote-ref-2)