Kesh Primary School

and

Kesh Community Nursery

Digital Safeguarding Policy

Reviewed in: November 2021

Ratified by the Board of Governors on: 18 November 2021

Next Review in: November 2024

Table of Contents

1. Rationale

The rapidly changing nature of the Internet and new technologies means that Digital Safeguarding and Internet Safety is an ever growing and changing area of interest and concern. The school has a duty of care to enable pupils to use on-line systems safely. This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. It is the wider duty of care to which all who work in schools are bound. It covers not only digital and internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The School must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. Digital Safeguarding and Internet Safety Policy that follows, explains how we intend to do this, while also addressing wider educational issues in order to help young people, parents / carers and school staff to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

This policy should be read alongside the following school policies: Positive Behaviour and Anti-Bullying Policy, Safeguarding and Child Protection Policy, Health and Safety Policy, Data Protection Policy and the UICT Policy.

2. Introduction

This document sets out the policy and practices for the safe and effective use of the Internet and digital technologies in Kesh Primary School and Community Nursery and is brought to the attention of all stakeholders.

We aim to develop mature systems of Digital and Internet Safety awareness, so that users can easily adapt their behaviours and become responsible users of any new technologies. As new technologies are developed, the school will endeavour to respond quickly to any potential Internet Safety threats posed by their use.

This policy is largely based on DENI Circular 2007/1 *'Acceptable Use of the Internet and Digital Technologies in Schools' and DENI Circular 2011/22 'Internet Safety Guidance'; 'Online Safety 2016/27; and adherence given to Circular 2017/04 – 'Safeguarding and Child Protection in Schools - A Guide for Schools' and* should also be read in conjunction with the School's Safeguarding policies. It has taken into account the recommendations of the *360 Degree Safe Internet Safety Self Review Tool*. The school has achieved the Digital School Award in recognition of its efforts to the promotion of safe and effective digital use.

This policy applies to all members of the School community who have access to and are users of the school ICT systems, both in and out of the School. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure the Digital Safeguarding and Internet Safety of all involved, apply sanctions as appropriate and review procedures.

In relation to digital and internet 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. Digital and internet 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 digital and internet safety incidents outside of the school, will be dealt with in accordance with School Policies.

3. Risk Assessment

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity, they will need to learn to recognise and avoid these risks — to become "Internet-wise" and ultimately good "digital citizens". Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online. The school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy.
DENI E-Safety Guidance, Circular number 2013/25

The main areas of risk for the School can be categorised as the Content, Contact, Conduct and Commercial activity.

Content

- Access to illegal, harmful or inappropriate images or other content.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.

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.

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.

Commercial

- The young child is exposed to inappropriate commercial advertising
- Exploitation due to marketing schemes and/or hidden costs/frauds

Many of these risks reflect situations in the offline world and it is essential that this Digital Safeguarding and Internet Safety Policy is used in conjunction with other School policies including Positive Behaviour and Anti-Bullying Policy, Safeguarding and Child Protection Policy, Health and Safety Policy, Data Protection Policy and the ICT Policy.

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.

What is Digital Safeguarding and Internet Safety?
Digital Safeguarding and Internet Safety in the school context:

- is concerned with safeguarding children in the digital world, with an emphasis on learning to understand and use technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

UICT is a compulsory cross-curricular element of the NI Curriculum and the school must ensure acquisition and development by pupils of these skills. The Internet and digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The school provides pupils with opportunities to use the excellent resources, along with developing the skills necessary to access, analyse and evaluate them.

4. Roles and Responsibilities

The policy has been drawn up by the School's UICT Team. The policy has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested. The policy and its implementation will be reviewed in 3 years or earlier if deemed necessary.

The Digital Safeguarding and Internet Safety Coordinator will lead the Internet Safety Team and takes day to day responsibility for Digital Safeguarding and Internet Safety issues and has a leading role in establishing and reviewing the Schools policies/documents.

The Digital Safeguarding and UICT team will:

- Ensure that all staff are aware of the procedures that need to be followed in the event of a Digital Safeguarding or Internet Safety incident taking place.
- Provide training and advice for staff/volunteers
- Liaise with C2K and school ICT technical staff

- Liaise with the EA and DENI on Digital Safeguarding and Internet Safety developments
- Liaise with the technical staff
- Receive reports of Digital Safeguarding and Internet Safety incidents and create a log of incidents to inform future Digital Safeguarding and Internet Safety developments
- Attend relevant meetings with Board of Governors
- Discuss current issues, review incident logs
- Monitors and reports to senior staff any risks to staff of which the E-Safety coordinator is aware
- Recruit, train and meet with Digital Leaders regularly (Yr5-Yr7)

Members of the UICT Team will assist with:

- The production and review of the school Digital Safeguarding and UICT policies and related documents.
- Mapping and reviewing the Digital Safety curricular provision, ensuring relevance, breadth and progression
- Monitoring incident logs from the pastoral team
- Consulting parents/carers and the pupils about the Digital Safety provision

The Designated Child Protection Teacher

The Child Protection Officer, *Mrs D Irvine,* will be skilled in Internet 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 incidents

The Principal and Senior Management Team

The Principal, has a duty of care for ensuring the safety (including Digital Safeguarding and Internet Safety) of members of the school community though the day-to-day responsibility for Digital Safeguarding and Internet Safety will be delegated to the Internet Safety Team.
The Principal, SMT and Digital Safeguarding and Internet Safety Teacher will be kept informed about Internet Safety incidents.
The Principal will deal with any serious Internet Safety allegation being made against a member of staff.
The Principal and SMT are responsible for ensuring that the Digital Safeguarding and Internet Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Internet Safety roles and to train other colleagues, as relevant.

Governors

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

Mrs E Milligan has taken on the role of Internet Safety Governor.

The designated Internet Safety Governor will:

- Liaise regularly with the Digital Safeguarding and UICT Team
- Regularly monitor Internet 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 Manager – *Mrs D Irvine*

The Network Manager will monitor that C2K Internet Safety measures, as recommended by DENI, working efficiently within the school to ensure that:

- The 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 Internet 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
- That they keep up to date with Digital Safeguarding and Internet Safety technical information in order to effectively carry out their Internet 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
- The "administrator" passwords for the school ICT system, used by the Network Managers are 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 an up-to-date awareness of Digital Safeguarding matters and of the current school Digital Safeguarding Policy and practices.
- They have read, understood and signed the school's Staff Acceptable Use Policy.
- They follow the school Digital Safeguarding Acceptable Use Policy.
- They report any suspected misuse or problem to the Digital Safeguarding and UICT Team.
- Digital communications with students (email / Virtual Learning Environment (VLE/Hubs) should be on a professional level only carried out using official school systems. Emails should be sent in accordance with the School's guidance.
- Digital Safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils have an understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act (1998)
- They monitor UICT activity in lessons, extracurricular and extended school activities. (Eg. Shared Education sessions).
- They are aware of Digital Safeguarding 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 Digital Safeguarding and UICT training as organised by the school

Professional Development for Teaching and Support Staff

Training will be offered as follows:

- All new staff will receive Internet Safety training as part of their Induction Programme, ensuring that they fully understand the school Digital Safeguarding Policy and Acceptable Use Policies.
- A programme of Internet Safety training will be made available to staff as an integral element of CPD. Training in Internet Safety will be supported where staff have identified a need.
- Staff will be made aware of the importance of filtering systems through the Internet Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
- This Digital Safeguarding Policy and its updates will be presented to and discussed by staff in staff meetings /Training days

Pupils as Digital Leaders
The Digital Leaders will assist with:

- Identifying/Reporting Potential issues regarding internet safety
- Presentation of information to the rest of the school during assemblies
- Ensuring messages are relayed to classes.
- Helping to organise Internet Safety events and campaigns.

Pupils
Are responsible for ensuring that:

- They use the school ICT systems in accordance with the Pupil Acceptable Use Policy which they will be expected to sign before being given access to school's systems.
- They have a good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.
- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They know and understand school guidelines and procedures on the use of iPads, mobile phones, digital cameras 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 'netiquette' of using e-mail both in school and at home.
- They understand the importance of adopting good Digital Safeguarding practice when using digital technologies out of school and realise that the school's Digital Safeguarding Policy covers their actions out of school, if related to their membership of the school.

5. Digital Safeguarding Education

We believe that, alongside a written Digital Safeguarding Policy and Codes of Practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication, both inside school and outside school. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

Digital Safeguarding education for pupils will be provided in the following ways:

- The Digital Leaders will lead a Digital Safeguarding assembly. All classes will be involved. The Digital Leaders will plan and organise the activities. They circulate Digital Safeguarding guidance to parents. They will test and review apps, receive technical training, help to train and assist staff and other classes; share ICT skills and provide technical support.
- A planned Digital Safeguarding curriculum is delivered as part of their lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Child Exploitation and Online Protection (CEOP) resources will be used as a teaching tool.
- 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 the student Acceptable Use Policy and 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 will be vigilant in monitoring the content of the websites the pupils visit.
- Pupils will be made aware of the importance of filtering systems through the Internet Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Other Resources:
Child Exploitation and Online Protection (CEOP) resources: a useful teaching tool looking at Internet safety and incorporated into our PDMU and UICT curriculums.

Childnet International www.childnet.com has produced materials to support the teaching of Internet Safety at Key Stage One and Two. They have materials for parents and staff too.

Other pupil resources available:

360 e Safety Tool, *Signposts to Safety, KidSMART, Know IT All for Schools, ThinkUKnow and Twinkl.*

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 Digital Safeguarding Policy outlined by the School.

Parents and Carers will be encouraged to support the school in promoting good Internet Safety practice and to follow School's guidelines on the appropriate use of:

- digital and video images taken at school events
- online communication with staff
- their children's use of personal devices in and out of school

Parents and 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:

- The school website www.keshprimary.co.uk provides links to external sites such as CEOP and Digital Parenting
- Letters, newsletters, websites and Digital Parenting leaflets
- Internet Safety Guidance will be delivered through key events

Digital Safety Awareness for Staff/ Professional Development

Teachers are the first line of defence in digital safeguarding; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Digital Safeguarding training is therefore an essential element of our staff induction and part of an on-going Continuous Professional Development programme. Through our Internet Safety policy, the school can ensure that all reasonable actions are taken and measures put in place to protect all users.

The induction programme for new staff includes Digital safeguarding. The UICT Team keeps informed and updated on issues relating to Digital Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of the Department's policy and strategy on ICT use in teaching and learning and are updated in relation to relevant changes. Staff uphold copyright regulations and intellectual property rights.

The Child Exploitation and Online Protection Centre (CEOP) runs regular one-day courses for teachers in Northern Ireland. Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the *Thinkuknow website.*

Internet Awareness for Governors

The UICT Team keeps governors updated on Internet Safety and Internet Safety issues. The Board of Governors has appointed Mrs E Milligan as their representative on the school Internet Safety Committee.

Internet Safety Awareness for Parents/ Carers and the Community

The Code of Safe Practice for pupils and Acceptable Use Agreement is sent home at the start of each school year for discussion with their child and parental signature. This Internet Safety Policy and Internet Safety materials are available on the school website.

6. Internet Services and Technical Framework

Connectivity and Filtering

The school has one internet system in its infrastructure. Internet access is filtered for all users.

C2K

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

The service allows for Websense filtering giving the school flexible control. Internet use is monitored. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school principal. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal devices are allowed, C2K filtering will be applied that is consistent with school practice.

Some of the safety services include:

- Providing all users with unique user names and passwords
- Tracking and recording all online activity using the unique user names and passwords
- Scanning all C2k email and attachments for inappropriate content and viruses
- Filters access to web sites

Auditing and Reporting

Filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. 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 with the Principal and the ICT Coordinator.

They manage the school filtering by:

- Monitoring reports of the use of C2k which is 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 Digital Safeguarding and UICT Team

Staff and children have a responsibility to report immediately 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.

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

- Safeguarding team
- Digital Safeguarding Team
- Board of Governors committee
- External filtering provider/PSNI on request

7. Code of Safe and Acceptable Practice

When using the Internet, email systems and digital technologies, all users must comply with relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. Staff and pupils are made aware that use of the school's ICT resources is a privilege which can be removed.

The school has:

(a) a Pupil Code of Safe and Acceptable Practice

(b) a Staff Code of Safe and Acceptable Practice

These contain Digital Safeguarding and Internet Safety Rules which makes explicit to all users what is safe and acceptable and what is not.

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

The Digital Safeguarding and Internet Safety Co-ordinator and the Senior Management Team will monitor the effectiveness of the Codes of Practice, particularly in the light of new developments in technology.

7a. Code of Safe and Acceptable Practice for Pupils

A parental/carer consent letter, accompanied by the Code of Safe and Acceptable Practice for pupils, is issued to parents/carers at the beginning of the new school year. This consent must be obtained before the pupil accesses the internet.

The following key measures have been adopted to ensure pupils do not access any inappropriate material:

- The Code of Safe and Acceptable Practice is made explicit to all pupils;
- Digital Safety guidelines are displayed prominently throughout the school
- Parents/Carers are asked to sign the Code of Safe and Acceptable Practice having discussed it with their child
- Pupils, using the Internet, will be working in highly-visible areas of the school
- All online activity is for appropriate educational purposes and supervised, where possible

- Pupils will, wherever possible, use sites pre-selected by the teacher and appropriate to age group
- Pupils are educated in the safe and effective use of the Internet, through a number of selected websites and resources.

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

Use of mobile phones by pupils is not permitted on the school premises during school hours.

7b. Code of Safe and Acceptable Practice for Staff

It is vital that staff adhere to the *GTCNI Code of Values and Professional Practice*. Staff are given computers, iPad, email and Internet access to assist them in the performance of their work. Staff should have no expectation of privacy in anything they create, store, send or receive using the school computer equipment (including iPads). The computer/iPad network is the property of the school and may only be used for school purposes. The school reserves the right to access activity and staff/pupils should be aware that improper use can lead to disciplinary action.

- Pupils accessing the Internet should on the whole be supervised by an adult at all times.
- Staff will make pupils aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to Mr Stewart, Mrs Irvine or Mrs Cullen.
- Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- Staff should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of pupils should, where possible, be taken with school equipment and images stored on a teacher iPad and/or the C2K 'Staff' storage area, accessible only to staff or under supervision for pupil work.
- School systems may not be used for unauthorised commercial transactions.
- Staff are expected to have secure passwords which are not shared and changed periodically.
- A Staff Safe and Acceptable Practice Code of Conduct, which details sanctions, is signed by all staff.

8. Health and Safety

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 the ICT Suite which has been designed in accordance with health and safety guidelines and where pupils are supervised at all times. Guidance is issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

Use of Mobile Phones

Most mobile phones have internet connectivity. Please refer to the schools Mobile Phone and Digital Technologies Policy for full guidance on the use of such. However, it must be noted that pupils do not bring mobile phones to school without the prior authorisation of their class teacher or Mr Stewart. In exceptional circumstances when the child is permitted a mobile phone in school, it will be handed to the class teacher and kept in a safe place until the end of the school day.

Digital and Video Images

Parental permission is gained when publishing personal images on the website, School Social Media platforms or other publications. All members of the school understand their rights and responsibilities in the taking, use, sharing, publication and distribution of images (and in particular the risks attached). The school gains parental/carer permission for use of photographs or video images. Staff are allowed to take images to support educational aims, Staff must follow school policies concerning the distribution and publication of such. Pupil surnames associated with images will not be shared. Digital images are securely stored on a teacher iPad or the central 'Staff' area and disposed of in accordance with the Data Protection Act. Parents sign to ensure digital images captured during school events are not to be published on a public platform if they depict the image of children other than their own.

Wireless Networks

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available on The Health Protection Agency website.

Personal Data

The school ensures all staff know and understand their obligations under the GDPR policy and comply with these to ensure the safe keeping of personal data, minimising the risk of loss or misuse of personal data. Staff have enhanced password protection with at least one capital letter and one number.

Data Protection Act

Staff are regularly reminded of Data Protection

In particular staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss and nature
- Ensure they are properly logged off at the end of a session and devices are password protected
- Transfer personal data using encryption and secure password protected devices
- Data is securely deleted from the device once it has been transferred or its use is complete.

Cloud Storage

Photographs and information is stored on the Cloud (Google Drive), meaning it can be securely accessed from any location removing the need to carry data and files on insecure data pens and portable devices.

CCTV

CCTV surveillance is in operation on the site. Recordings will not be revealed without permission, except to the PSNI for a criminal investigation.

Cyber Bullying

Staff are made aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is considered within the schools overall Anti-Bullying policy and Positive Behaviour Policy as well as the Digital Safeguarding Policy.

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 occurs 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.
- Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator. Pupils will be reminded that cyber-bullying can constitute a criminal offence.
- Cyber-bullying is addressed within the school’s Anti-bullying ethos via regular class and whole school events. It also is dealt with within our PDMU and PATHS curriculums.

While there is no specific legislation for cyber-bullying, the following covers different elements of cyber-bullying behaviour:

Protection from Harassment (NI) Order 1997	http://www.legislation.gov.uk/nisi/1997/1180
Malicious Communications (NI) Order 1988	http://www.legislation.gov.uk/nisi/1988/1849
The Communications Act 2003	http://www.legislation.gov.uk/ukpga/2003/21

Pupils are encouraged to report incidents of cyber-bullying to their parents and the school. If appropriate, the PSNI may be informed to ensure the matter is properly addressed and behaviour ceases. The school will keep records of cyber-bullying incidents on SIMS to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

School Website and Social Media Platforms

The school website www.keshprimary.co.uk and Social Media Platforms are used to celebrate pupils' work, promote the school and provide information. The website reflects the school's ethos. Information is accurate and well presented and personal security is not compromised.

The following rules apply:

- The point of contact is the school address, school e-mail and telephone number.
- Staff or pupils' home information will not be published.
- Photographs that include pupils will be selected carefully. Parents who prefer their child’s photographs to not appear is respected.
- Pupils' full names will not be used in association with photographs; parents’ permission will be sought if names are to accompany to accompany special photographs such as personal awards.
- The Principal will take overall editorial responsibility and ensure content is accurate and appropriate.

Social Media on the C2K System

Community networks, chatrooms, instant messenger systems, online journals, social networks and blogs, enable sharing of resources, ideas, pictures and video amongst users, the majority of which, usually causes no concern. Concern, in relation to inappropriate activities, tends to emanate from use outside school. C2k filters out social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment.

Safe and responsible use of social media is addressed through our Digital Safeguarding Education Programmes. We make staff, pupils and parents aware of the risks associated with the use of social media and encourage responsible use outside school. Information and education is provided for parents on the school website, school newsletter and at parent and community internet safety meetings. Instances of pupil/staff cyber bullying will be regarded as serious offences and dealt with according to the school's discipline policy and child protection procedures.

Actions and Sanctions

- Pupil Incidents

We believe it is important that the school has a culture under which users understand and accept the need for Digital Safeguarding regulations and adopt positive behaviours, rather than one in which attitudes are determined solely by sanctions.

- Reporting Pupil Incidents

Users will understand their responsibilities to report Digital Safeguarding incidents. They will know and understand that there are clear systems for reporting abuse and understand that the processes must be followed rigorously.

Incident reports will be logged for future auditing, monitoring, analysis and for identifying serious issues or patterns of incidents. This will allow the school to review and update Digital Safeguarding Policy and practices.

Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately. Users will have an understanding of how to report issues online, including to CEOP.

Staff Incidents and Reporting

All new staff, volunteers and students on work experience are provided with an induction programme. This includes Child protection and Safeguarding, code of conduct and e-safety.

The Code of Conduct is brought to all staff on an annual basis. All staff are asked to read through the code of conduct and sign on an annual basis. Any breach of the staff code of conduct, Internet Safety or social media policy will be dealt with by the principal and/or governors.

- Staff Sanctions

Governors will deal with breaches of policy by the staff.

Governors will refer to the DE Governor's Handbook.

Governors will take advice from appropriate authorities.

Governors will follow the EA Disciplinary Guidelines.

Kesh Primary School and Community Nursery

44 Crevenish Road, Kesh, Co Fermanagh, BT93 1RF

Email : bstewart413@kesh.enniskillen.ni.sch.uk

Tel: 028 68631441

www.keshprimary.co.uk

Dear Parent/ Carer

It is essential that pupils are aware of Internet Safety and know how to stay safe when using Information and Communications technology (ICT). As part of Kesh Primary School and Community Nursery's UICT programme, we offer pupils supervised access to a *filtered* Internet service provided by C2k. Access to the Internet enables pupils to explore and make appropriate use of many websites that are of enormous educational benefit. They can also exchange messages with other Internet users throughout the world. However, in spite of the tremendous learning potential, you should be advised that some material accessible, via the Internet, may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service providers C2k have installed filtering software which operate by blocking thousands of inappropriate websites and barring inappropriate items, terms and searches in both Internet and e-mail.

To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

We would also like to remind you that any digital images taken at school events, and place on social media, must only display **your own** child/children.

The school's Acceptable Use of the Internet Policy for Pupils is printed on the back of this letter. These have been differentiated according to the age of your child. Please read these with your child and return the slip at the bottom of the page.

If you have any concerns or would like some explanation, please contact your class teacher.

- -✂- -

Parent/ Carer signature

Pupil: _________________ Class: ___________________

We have discussed the information and ……………………………………….... (child's name) agrees to follow the Acceptable Use of the Internet Policy and to support the safe use of ICT at Kesh Primary School and Community Nursery

Parent/ Carer's Signature ………………………………………………… Date ……………………………………..………

Kesh Primary School and Community Nursery

44 Crevenish Road, Kesh, Co Fermanagh, BT93 1RF

Email : bstewart413@kesh.enniskillen.ni.sch.uk

Tel: 028 68631441

www.keshprimary.co.uk

Acceptable Use Policy – Year 1 and Year 2

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computers / tablets.
- I will only use activities on the computer / tablet that an adult has told me I can use.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I think something is wrong on the computer / tablet.
- I will tell an adult if I see something that upsets me on the computer / tablet.
- I know that if I break the rules I might not be allowed to use a computer / tablet.

Parent/ Carer's Signature ……………………………………………… Date ……………………………………………

Kesh Primary School and Community Nursery

44 Crevenish Road, Kesh, Co Fermanagh, BT93 1RF

Email : bstewart413@kesh.enniskillen.ni.sch.uk

Tel: 028 68631441

www.keshprimary.co.uk

Acceptable Use Policy - Year 3 and Year 4

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computers / tablets.
- I will only log onto the *My School* learning platform using my own username and password
- I will only use activities on the computer / tablet that an adult has told me I can use.

- I will be kind and considerate when using ICT for communication
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I think something is wrong on the computer / tablet.
- I will tell an adult if I see something that upsets me on the computer / tablet.
- I will be responsible for my behaviour when using ICT because I
- I know that if I break the rules I might not be allowed to use a computer / tablet.

Parent/ Carer's Signature ……………………………………………… Date ………………………………………………

Kesh Primary School and Community Nursery

44 Crevenish Road, Kesh, Co Fermanagh, BT93 1RF

Email : bstewart413@kesh.enniskillen.ni.sch.uk

Tel: 028 68631441

www.keshprimary.co.uk

Acceptable Use Policy - Year 5, Year 6 and Year 7

I understand that I must use computers and the internet in a responsible way to ensure that there is no risk to my safety. This is how we stay safe when using computers and devices.

- I understand that adults in school will monitor my use of the computer, digital devices and the internet.
- I will keep my username and password safe. I will not share it or use any other person's username and password. I understand that I should not store a password where it is possible that someone may see it.
- I will keep safe when I am on-line by following the 'SMART' and 'SAFE' rules displayed the Computer Room and classrooms.
- I will not share personal information about myself or others when online (which could include names, addresses, email addresses, telephone numbers, age, school address, passwords etc.).
- I will tell an adult about anything that makes me unsafe or feel uncomfortable online.
- I understand that the computers and devices in school are mainly to be used for learning and that I will not use them for personal or leisure use.
- I will be polite and responsible when I communicate with others online unless I have permission.
- I will not knowingly search for, or open games/sites which are not appropriate for me
- I not will use my own personal devices (mobile phones / USB devices etc.) in school, unless I have permission.
- I understand the risks of uploading information and will not try to upload or download anything in school.
- I will tell an adult about any damage or faults with computers or devices.
- I will not open any links in emails or any attachments to emails, unless I know and trust the person that sent the email.
- I understand that I am responsible for my actions, both in and out of school and if I fail to follow the Acceptable Use Policy rules I may lose my access to the school computer and internet.

Parent/ Carer's Signature ……………………………………………………   Date ……………………………………………….

Code of Safe and Acceptable Practice (Staff)

Code of Safe and Acceptable Practice-
Mobile Phones, Digital Devices and Internet Infrastructure

At Kesh Primary School the welfare and well-being of our pupils and staff is paramount. The aim of the Use of Mobile Phones and Digital Devices Policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable digital device user guidelines.
This is achieved through balancing protection against potential misuse with the recognition that mobile devices are effective communication tools. It is recognised that it is the enhanced functions of many mobile phones that cause the most concern, offering distractions and disruption to the working day, and which are most susceptible to misuse – including the taking and distribution of indecent images, exploitation and bullying. However, as it is difficult to detect specific usage, this policy refers to ALL mobile communication devices.

Code of Conduct

A code of conduct is promoted with the aim of creating a cooperative workforce, where staff work as a team, have high values and respect each other; thus creating a strong morale and sense of commitment leading to increased productivity. Our aim is therefore that all practitioners: -

- Have a clear understanding of what constitutes misuse
- Know how to minimise risk
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to possible allegations
- Understand the need for professional boundaries and clear guidance regarding acceptable use
- Are responsible for self-moderation of their own behaviours
- Are aware of the importance of reporting concerns promptly

It is fully recognised that imposing rigid regulations on the actions of others can be counterproductive however an agreement of trust is therefore promoted regarding the carrying and use of mobile phones within the setting, which is agreed to by all users.

Personal Mobiles – Staff

- Staff are not permitted to make/receive calls/texts/engage on social media during contact time with children or whilst carrying out school duties (preparing work, photocopying, marking etc.)

School related calls should be made via landlines located in each classroom and/or via the school office.
. If you are in a location where communication is not possible (e.g. School Trip/Sporting event) staff should carry mobile phones for emergency use only.

- Staff should have their phones on silent or switched off and out of sight (e.g. in a drawer, handbag) during class time.
- Mobile phones should not be used for any purpose in a space where children are present (e.g. classroom, corridor, playground).
- Use of phones (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- Staff must security protect access to their phone.
- Should there be exceptional circumstances (e.g. acutely sick relative), then staff should make the Principal aware of this so exceptions can be made.
- Staff are not at any time permitted to use recording equipment on their mobile phones, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras and iPads.
- Staff should report any usage of mobile devices that causes them concern to the Principal.

Mobile Phones for work related purposes

We recognise that digital devices provide a useful means of communication during off-site activities. However, staff should ensure that: -

- Mobile use on these occasions is appropriate and professional (and will never include taking photographs of children)
- Mobile phones should not be used to make contact with parents during school trips unless in an emergency situation – all non-emergency communications should be made via the School Office when possible.
- Where parents are accompanying trips they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone to take photographs of children.

Use of the School ICT Equipment and Internet Infrastructure

- EMAIL: I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors. I will use the approved C2k secure e-mail system for school business. I will ensure that all electronic communications with staff are compatible with my professional role.
- PASSWORDS: I will comply with the C2K UICT system security and not disclose passwords provided to me by the school or other related authorities.
- DATA PROTECTION: I will not give out personal details e.g. mobile phone number/personal e-mail/School e-mail address to pupils or to parents to conduct any school related business. I will ensure personal data is kept secure and used appropriately, whether in school, taken off school premises or accessed remotely. Personal data will only be taken out of school or accessed remotely when authorised by the Principal. Such data must be encrypted. Images of pupils/staff will only be taken, stored and used for professional purposes online using a school iPad. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Principal.
- C2K INSTALLATION: I will not install any hardware or software on the C2K system without permission from the E-Safety team.

- USE OF INTERNET AND DEVICES: I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory on the C2K system or iPads. I understand that my use of the Internet and other related technologies can be monitored and logged and can be made available, on request. I will respect copyright and intellectual property rights.
- I will support and promote the school's Internet Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

Signed ___________________________ Chairman of Board of Governors

___________________________________ Principal

Date: 18th November 2021

Involved in the consultation of the policy - All members of the teaching staff
Shared with staff – November 2021
Review Date – November 2024

Keep Our iPads

Stay away from liquids

Always use two hands

Follow instructions

Enjoy this technology & treat it with respect!

This is how I stay safe when I use the iPad:

- ✓ I will protect the iPad and carry it carefully in its case
- ✓ I will keep food and drinks away from the iPad as they may damage it
- ✓ I will not change the settings on the iPad without adult permission
- ✓ I will only use activities on the iPad that a teacher/classroom assistant had allowed me to use
- ✓ I will tell a teacher or classroom assistant if I see something that upsets me on the screen
- ✓ I will use the camera when the teacher tells me and photograph people with permission
- ✓ I will never share images or movies on the internet, unless I am instructed to by my teacher
- ✓ I will abide by the school’s Internet Safety rules

I know that if I break the rules, I might not be allowed to use the iPad for some time.

S Keep Safe...

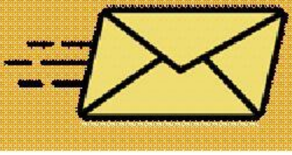
Never tell someone on the internet or on a mobile phone your full name, your address or your telephone number.

M Never Meet...

Never meet up with an online friend. If somebody asks to meet you, tell an adult. **Never** go alone.

A Never Accept...

Never accept emails or text messages from people you do not know.



R Reliable...

Never rely on what you see on the internet. It's not always true. Don't rely on people you meet online they may lie about who they are.

T Always Tell...

Always tell an adult if somebody upsets you. Tell and adult if you see something on the computer that makes you sad.

Use of ALL digital images agreement

As part of our Digital Safeguarding Policy we require that digital images, captured by parents/guests during school events, featuring children other than their own are NOT displayed on **any** Social Media or public platform.

(Date and time)

(Event)

Print Name	Signature	Digital images taken Please tick)