HOLLYBANK PRIMARY SCHOOL

Online Safety Policy

Date of Next Policy Review	**February 2023**
Name of Person Responsible for Policy	**N CULBERT**
Issued to	**Staff, Parents and Governors**
Date of Issue	**February 2021**

What is Online Safety?

Online safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

Online safety in the school context is:

- ✓ Concerned with safeguarding children and young people in the digital world and emphasises learning to understand and use technologies in a positive way
- ✓ Less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online
- ✓ Concerned with supporting pupils to develop safer online behaviours both in and out of school
- ✓ Concerned with helping pupils recognise unsafe situations and how to respond appropriately.

The rapidly changing nature of the Internet and new technologies means that online safety is an ever growing and changing area of interest and concern. This Policy reflects this by keeping abreast of the changes taking place. The school has a duty of care to enable pupils to use online systems safely. This policy is based on and complies with DENI Curricular 2007/1 on Acceptable Use of the Internet and Digital Technologies in School and DENI Circulars 2011/22, 2013/25 and 2016/27 on Online Safety.

Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

- ✓ Websites
- ✓ Learning Platforms and Virtual Learning Environments
- ✓ Email and Instant Messaging
- ✓ Social Networking
- ✓ Blogs and Wikis
- ✓ Podcasting
- ✓ Video Broadcasting
- ✓ Music Downloading
- ✓ Gaming
- ✓ Apps
- ✓ Mobile/Smart phones with text, video and/or web functionality
- ✓ iPads, tablets and other mobile devices with web functionality

The DENI circular 2007/01 states that:

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

In Hollybank Primary School we understand the responsibility to educate our pupils in online safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Using the Internet for Education

The benefits include:

- ✓ access to a wide variety of educational resources, including online assessment:
- ✓ rapid and cost-effective communication.
- ✓ gaining an understanding of people and cultures around the globe.
- ✓ staff professional development through access to new curriculum materials, shared knowledge and practice.
- ✓ greatly increased skills in Literacy, particularly in being able to read and appraise critically and then communicate what is important to others.
- ✓ social and leisure use.

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications channel, available to all. Anyone can send messages, discuss ideas, and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials, some of which could be unsuitable.

The rapidly changing nature of the Internet and new technologies means that Online Safety is an ever growing and changing area of interest and concern. This Online Safety policy reflects this by keeping abreast of the changes taking place. Schools have a duty of care to enable pupils to use on-line systems safely.

This Online Safety policy operates in conjunction with other school policies including:

- ✓ Positive Behaviour
- ✓ Child Protection
- ✓ Anti-Bullying
- ✓ Acceptable Use of Mobile Phones and other Related Technologies
- ✓ Seesaw Policy
- ✓ Blended and Remote Learning Policy

Online Safety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the Northern Ireland curriculum and schools must ensure acquisition and development by pupils of these skills.

This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Online Safety in Hollybank Primary School depends on effective practice at several levels:

- ✓ responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- ✓ sound implementation of the Online Safety Policy in both administration and curriculum, including secure school network design and use;

- ✓ safe and secure internet provision by C2K.

Concerns are:

Potential Contact

Children may encounter someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons

Children should be taught:

- ✓ That people are not always who they say they are.
- ✓ That "Stranger Danger" applies to the people they encounter through the Internet.
- ✓ That they should never give out personal details
- ✓ That they should never meet anyone contacted via the Internet
- ✓ That once they publish information it can be disseminated with ease and cannot be destroyed.

Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet.

Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content.

Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.

Materials may contain misleading and inaccurate information. E.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

Children should be taught:

- ✓ That information on the Internet is not always accurate or true.
- ✓ To question the source of information.
- ✓ How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

- ✓ Not to fill out forms with a lot of personal details.
- ✓ Not to use an adult's credit card number to order online products.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

Cyber Bullying

Staff at Hollybank Primary School are aware that pupils may be subject to cyber bullying via electronic methods of communications both in and out of school. This form of bullying is addressed within our school's Anti-Bullying Policy and Child Protection and 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 and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity
- ✓ Social Networking Sites – Typically includes posting or publication or 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 include abusive texts, videos or photo messages
- ✓ Abusing Personal Information – May include the posting of photos, personal information, fake comments and blogs or pretending to being someone online without that person's permission.

Whilst cyber-bulling may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber bullying can constitute a criminal offence.

Our pupils are encouraged to report incidents of cyber-bullying to their parents and the school. The school will keep records of any cyber bullying reported to them in the Online safety Concerns Book kept in the Principal's Office. (Appendix 1)

Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current Online Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of Online Safety throughout the school.

The Principal/ICT Co-ordinator will update School Leadership and Governors regarding online safety and all governors should understand the issues at our school in relation to local and national guidelines and advice.

C2K

Classroom 2000 (C2K) is the project responsible for the provision of Information and Communications Technology (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.

Some of these safety services include:

- ✓ Providing all users with unique usernames and passwords
- ✓ Tracking and recording all online activity using the unique usernames and passwords
- ✓ Scanning all C2k email and attachments for inappropriate content and viruses.
- ✓ Filters access to web sites
- ✓ Providing appropriate curriculum software.

Should the school decide to access online services through service providers other than C2K then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.

Responsibilities:

Role		Contact Details
Online Safety Team	**Miss L. Brett / Mrs N.Culbert**	
ICT Co-ordinator/ E-Safety Co-ordinator	**Mrs N. Culbert**	**nculbert830@c2kni.net 02890 864944**
Online Safety Governor		
Designated Child Protection Teacher	**Mrs N. Culbert**	**nculbert830@c2kni.net 02890 864944**
Deputy Designated Child Protection Teacher	**Miss L. Brett**	**lbrett508@c2kni.net 02890 864944**
Designated Governor for Child Protection	**Mrs V. Robinson**	

Online Safety Team

Our Online Safety Team is responsible for the day-to-day issues relating to Online Safety.

The e-Safety co-ordinator:

- ✓ leads discussions on Online Safety with the School Council;
- ✓ takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies/documents;
- ✓ ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident.
- ✓ provides training and advice for staff;

- ✓ liaises with the Education Authority;
- ✓ receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments; (Appendix 1)
- ✓ reports regularly to Senior Management Team;
- ✓ receives appropriate training and support to fulfil his/her role effectively;

The Board of Governors:

- ✓ are responsible for the approval of this policy and for reviewing its effectiveness. The governors should receive regular information about e-Safety incidents and monitoring reports.

The Principal:

- ✓ is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day-to-day responsibility for Online Safety is delegated to the Online Safety co-ordinator; and the Vice-Principal should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Refer to staff disciplinary procedures, and/or Child Protection/Safeguarding Children Policy.

Teaching and Support Staff must:

- ✓ have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices.
- ✓ embed Online Safety issues into the curriculum and other school activities as appropriate.
- ✓ have read, understood, and signed the school's Acceptable Use of the Internet for staff; (Appendix 2)
- ✓ report any suspected misuse or problem to the school's Online Safety co-ordinator.

Online Safety Skills' Development for Staff

- ✓ All staff receive regular information and training on Online Safety issues through the co-ordinator at staff meetings.
- ✓ All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- ✓ New staff members receive information on the school's Acceptable Use Agreement as part of their induction. (Appendix 2)
- ✓ All staff are encouraged to incorporate Online Safety activities and awareness within their lessons. Lessons for each year group are available within Staff Folder on School Drive. Google Be Internet Legends scheme of Work and Digital Wellbeing Lessons are shared with staff regularly.

Community Use of School ICT Resources

The school's ICT facilities can be used as a community resource under the Extended Schools programme. Users are issued with separate usernames and passwords by C2K. They must also agree to the school's Acceptable Use of the Internet policy before participating and only access pre-selected and appropriate websites.

Teaching and Learning

Internet use:

The school will plan and provide opportunities within a range of curriculum areas to teach Online Safety. Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.

Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies, i.e. parent/carer, teacher/trusted member of staff, or an organisation such as C2k / UK Safer Internet Centre.

The school Internet access is filtered through the C2k managed service. No filtering service is 100% effective; therefore, all children's use of the Internet is supervised by an adult. Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval, and evaluation.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

Pupils in Key Stage 1 and 2 are educated in the safe and effective use of the Internet, by the PSNI, INEQE, Women's Aid and the NSPCC. P7 pupils participate in a 'Bee Safe' event in conjunction with local council and the PSNI which includes information on how to stay safe online.

The use of mobile phones by pupils is not permitted on the school premises. During school hours pupils are forbidden to play computer games or access social networking sites.

The school's Online Safety SMART rules for use of the Internet and other digital technologies is made explicit to all pupils and are displayed prominently throughout the school.

iPad use:

Apps are downloaded by the ICT co-ordinator/Class Teacher. Pupils do not have the facility to download apps.

E-mail:

C2k recommends that all staff and pupils are encouraged to use their C2k email system for school business. It is strongly advised that staff should not use personal email accounts for school business. The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

Pupils must immediately tell a teacher if they receive offensive e-mail. The forwarding of chain mail is not permitted.

Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet.

Children are not always given individual e-mail addresses. In some instances, children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

Social Networking:

This is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks, video calling and blogs (personal web journals). Social environments enable any community to share resources and ideas amongst users. Such software allows users to exchange resources, ideas, pictures and video.

We regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils. Appropriate information and indeed education will also be provided for our parents.

The school C2k system will block access to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location. Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals. School staff will not add children as 'friends' if they use these sites.

Our pupils are asked to report any incidents of bullying to the school.

The use of social media sites (Eg., Facebook, Twitter, etc.) are now commonplace with the result that the lines between work and personal life can become blurred. To protect staff, pupils and the reputation of the school the following guidelines should be followed:

- ✓ Staff should not use the C2K system to engage in personal social media activities. This inappropriate use of social media sites may be treated as a disciplinary matter.

- ✓ If staff use social media sites for personal use, they are reminded that they have a responsibility to ensure they are posting comments or images that are not detrimental to their position as a member of staff of Hollybank Primary School, the privacy or rights of pupils or the reputation of the school.
- ✓ **A common sense approach to the use of social media websites is recommended**.
- ✓ Under no circumstance should offensive or discriminatory comments be made about work colleagues on the internet. This may amount to cyber-bullying or defamation and could be deemed a disciplinary matter.

Mobile Technologies:

The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material. Staff should not store pupils' personal data and photographs on memory sticks / mobile phones. Staff are being encouraged to make use of safe, secure online storage solutions such as Google Drive, meaning that sensitive data need not leave the school premises.

Staff members should where possible use school iPads to take photos or videos of children partaking in educational activities/trips. They may use personal digital cameras (on their phones or otherwise) on trips if necessary but any images must be quickly transferred back to the school system and deleted permanently from their personal camera.

We recognise that access to mobile phones by children has become a useful tool for families to keep in contact with each other in case of emergency on the way to and from school. However, if pupils bring mobile phones to school, the phones must remain switched off and kept out of sight while pupils are in class, the school building, the school grounds or during off site activities. Where a pupil is found by a member of staff to be using a mobile phone during the school day, the phone may be taken from the pupil and handed to a member of the school's Senior Leadership Team (SLT). The mobile phone will be stored in the school office until the end of the school day. The pupil may collect the phone at the end of the school day and the child's parent/guardian will be contacted.

Staff should not use personal mobile phones during designated teaching sessions or whilst supervising children unless for the purposes of school business. If a personal call needs to be taken, permission must be sought in advance from the Principal.

In light of new GDPR guidelines, any loss or breach of data must be reported immediately to the ICT-Co-ordinator and Principal.

Managing Video-conferencing:

Videoconferencing will be via the C2k network to ensure quality of service andsecurity. It will also be appropriately supervised.

Publishing Pupils' Images and Work

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website and Seesaw. This consent form is considered valid for the

entire period that the child attends Hollybank Primary School unless there is a change in the child's circumstances where consent could be an issue. Parents/carers may withdraw permission, in writing, at any time. (Appendix 4)

Pupils' full names will not be used anywhere on the School Website or Seesaw particularly in association with photographs.

Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Policy decisions:

Authorising Internet access:

- ✓ Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Pupils' Acceptable Use Agreement (Appendix 3) and abide by the school's online safety rules. These online safety (SMART) rules will also be displayed clearly in all rooms and discussed with the pupils. (Appendix 5). Foundation Stage Children will be introduced to Smartie the Penguin and follow his simple rules for keeping safe online. (Appendix 6)
- ✓ Access to the Internet will be supervised.
- ✓ All parents will be asked to sign the Pupils' Acceptable Use Agreement giving consent for their child to use the Internet in school by following the school's online safety rules and within the constraints detailed in the school's Online safety policy.
- ✓ All staff must read and agree in writing to adhere to the Staff Acceptable Use Agreement before using any school ICT resource. (Appendix 2)

Password Security:

- ✓ Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- ✓ All pupils are provided with an individual login username and password.
- ✓ Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- ✓ Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Handling online safety Complaints:

Pupils and parents will be informed of the complaints' procedure.

To deal with any incidents of technology misuse by pupils which arise, the school's Positive Behaviour Policy will be followed. Pupils must be made aware that repeated misuse of the Internet may lead to their access to it being denied. If a member of staff is involved, then the disciplinary procedures for employees of the school will be followed.

Where the incident involves child abuse, the Designated Teacher for Child Protection in the school must be notified and the school will follow procedures as set out in the school's Child Protection/Safeguarding Children Policy.

Issues of Internet misuse and access to any inappropriate material by any user should be reported immediately to the school's Online Safety Co-ordinator and recorded in the school's Online Safety log, giving details of the site and the time. (Appendix 1)

A record of very serious Online Safety incidents will be kept in the locked Child Protection cabinet within school and a Note of Concern Form completed. (see Child Protection Policy)

Harassment of another person using technology, or breaching their right to privacy (e.g. reading their mail, accessing their files, using their computer account or electronic mail address), poses a threat to their physical and emotional safety, and may have legal consequences. For these purposes, it is also essential that evidence of misuse is secured. If the school identifies a suspect device (containing for instance indecent images or offences concerning child protection), it will not be used or viewed, and advice will be sought from the P.S.N.I. After a minor or major incident, a comprehensive debriefing will occur to review school policy and procedures.

If police involvement is necessary, the Principal/Online Safety Team/Board of Governors will seek advice from Schools' Branch and the legal department at the Education Authority (North Eastern Region).

Introducing the Online Safety Policy to pupils and parents

Online safety rules (SMART) will be displayed in all classrooms and discussed with the pupils throughout the year. Specific lessons will be taught by class teachers during Anti-Bullying Week (term 1), on Safer Internet Day (term 2) and at a relevant point during term 3. They will also be incorporated into PDMU lessons throughout each term. An assembly will be led by the ICT Co-ordinator/Class Teacher on Safer Internet Day based on the given theme for the year.

As issues arise in the news etc they will be dealt with appropriately in school and information where possible will be given to parents to help them.

Pupils will be informed that network and Internet use will be monitored.

Online safety information will be included throughout the year in the school newsletter. Advise and relevant information will be sent home to parents on Safer Internet Day and as the need arises.

Online safety for Parents / Carers

- ✓ Parents/carers are asked to read through and explain the Pupil Acceptable Use Agreement (Appendix 3) to their child.
- ✓ Parents/carers are required to decide as to whether they consent to their child having access to the Internet for Educational purposes. (Appendix 4)
- ✓ Parents/carers are required to decide as to whether they consent to images of their child being taken/used on the school website and Seesaw (Appendix 4)

- ✓ The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.
- ✓ The school will communicate relevant online safety information through newsletters, Seesaw and the school website.
- ✓ Parents should remember that it is important to promote Online Safety in the home and to monitor Internet use.
- ✓ Keep the computer in a communal area of the home.
- ✓ Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- ✓ Monitor on-line time and be aware of excessive hours spent on the Internet.
- ✓ Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- ✓ Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART rules. (Appendix 5)
- ✓ Discuss the fact that there are websites/social networking activities which are unsuitable.
- ✓ Discuss how children should respond to unsuitable materials or requests.
- ✓ Remind children never to give out personal information online.
- ✓ Remind children that people online may not be who they say they are.
- ✓ Be vigilant. Ensure that children do not arrange to meet someone they meet online.
- ✓ Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.
- ✓ All parents must not post pictures of other children without consent on social media or share photographs/information from Seesaw on personal social media accounts.

Staff and the online safety Policy:

All staff will be given the School Online Safety Policy and its importance explained each year with the Child Protection training

Any information downloaded must be respectful of copyright, property rights and privacy.

Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct are essential.

A laptop or iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use regarding Internet access, data protection and use of software, both in and out of school.

Home Learning Platforms - Seesaw

All staff have been trained and given advice on how to effectively use Seesaw to enhance Teaching and Learning at home and for Remote/Blended Learning.

Parents will be informed about Seesaw and how it can enhance the learning of each child.

All children will be taught how to effectively use Seesaw to access learning outside of the classroom. They will be given a username and password/QR code to access individual learning resources and activities.

Seesaw and the blog linked to each class will be regularly monitored for incidents of cyberbullying, inappropriate use of language or the uploading of inappropriate files. (All comments/post require teacher approval.)

Children will be informed that the sending of messages through the Seesaw Blog is monitored and misuse of the commenting system will result firstly in a warning, followed by their ability to comment being removed should such behaviour be repeated.

Related policies:

- ✓ Seesaw Policy
- ✓ Blended and Remote Learning Policy

School Web Site

The school website is used to celebrate pupils' work, promote the school, and provide information. Editorial guidance will ensure that the Website reflects the school's ethos that information is accurate and well-presented, and that personal security is not compromised. As a teaching team we ensure common values and quality control. As the school's Website can be accessed by anyone on the Internet, the school must be very careful to safeguard the interests of its pupils and staff. The following rules apply:

- ✓ The point of contact on the Website will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- ✓ Website photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site (see Appendix 4).
- ✓ Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- ✓ Teaching staff will take overall editorial responsibility and ensure that content is accurate and appropriate.
- ✓ The Website should comply with the school's guidelines for publications.
- ✓ The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Health and Safety

In Hollybank Primary School 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 ICT suite, which has been designed in accordance with Health and Safety guidelines.

Pupils are always supervised when Interactive Whiteboards and Digital Projectors are being used. Guidance is also 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 also mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

Monitoring and Review

This policy is implemented on a day-to-day basis by all school staff and is monitored on an annual basis by the ICT Coordinator.

School Online safety is reviewed annually through the 360 safe School Online Safety Self Review Tool.

This document sets out the policy and practices for the safe and effective use of the Internet in Hollybank Primary School. The policy has been drawn up by the staff of the school under the leadership of Lynsey Brett/Naomi Culbert *(Principal/ICT Co-ordinator)*. It 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.

Appendix 1

Online Safety Concern

Date	Pupil Name	Online Concern	Action Taken

Appendix 2

Acceptable Use of the Internet and Digital Technologies

Staff/Volunteer

The computer system is owned by the school and is made available to all staff to enhance their professional activities including teaching, research, administration, and management. Teaching staff have been allocated a School iPad. The school's 'Acceptable Use of the Internet and Digital Technologies Policy' has been drawn up to protect all parties – the pupils, the staff, and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. In line with the school's Online Safety Policy, the following Code of Safe Practice has been highlighted and agreed to by all staff - Staff should sign a copy of this Code of Conduct and return it to the ICT Co-ordinator.

- ✓ Members of staff may be allocated access by the C2k manager (and with permission from the Principal) to a website that may potentially contain inappropriate content e.g. Youtube, Vimeo etc. Staff members should not search through these sites as this may provide opportunities for inappropriate content to be seen by pupils. Instead staff should preview whichever web page he/she wishes to use for educational purposes prior to class use.
- ✓ Staff should never accept a 'friend request' from a pupil on any social networking site, either inside or outside of school.
- ✓ Staff should never share their mobile phone number or personal email address with a pupil, either inside or outside of school.
- ✓ During working hours, all staff (teaching and non-teaching) should ensure that personal mobile phones are on 'silent' mode' during class teaching time.
- ✓ Staff should ensure that all pupils are aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils.
- ✓ Staff should ensure that all pupils using the Internet have written permission from their parents.
- ✓ Websites used by pupils should be checked beforehand by teachers, as far as is possible, to ensure that there is no unsuitable content, and that material is age-appropriate.
- ✓ Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/I.C.T. Co-ordinator.
- ✓ In the interests of system security, staff passwords should only be shared with the network manager. Substitute teachers should use their own username and password which is left for them by the relevant staff member.
- ✓ 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 members are advised to use their c2k email address and not their personal email address. This ensures that all activity can be easily monitored and that content is appropriate and virus free.
- ✓ Photographs of pupils should be taken with a school iPad. Consequently, staff should not take a photograph of a child with their personal mobile phone or store any images (or Child Protection Data) of any child on any personal laptop etc. However, in exceptional circumstances, with permission from the Principal, staff members may take photographs of children with their mobile phone. This may only be done in the understanding that such images are immediately transferred to the school network upon return to the classroom. In addition, the staff member is responsible for the subsequent and immediate deletion of such pictures/videos from the phone and any automatic online storage associated with the phone. e.g. if a camera has been forgotten on an educational visit
- ✓ As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- ✓ School systems may not be used for any unauthorised commercial transactions i.e. permission must be sought from the Principal
- ✓ Staff will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- ✓ Staff will respect copyright and intellectual property rights.
- ✓ Staff will ensure that any online activity, both in school and outside school, will not bring their professional role into disrepute.
- ✓ Staff **must immediately** report any illegal, inappropriate or harmful material or incident they become aware of, to the Principal or the school's ICT co-ordinator;

Confirmation of Compliance

I hereby confirm that I have read, understood and agree to comply with the school's Acceptable Use of the Internet and Digital Technology.

Name:

Position/Post Held:

Signed:

Date:

Once signed and dated, please return this form to the ICT Co-ordinator (Mrs N. Culbert).

Appendix 3

Acceptable Use of the Internet and Digital Technologies

Pupil

In Hollybank Primary School we use a networked computer system which is filtered and controlled by C2K. This system enables staff and pupils to share and store materials electronically and to access a limited number of Internet sites which are of educational value.

Children will only access the filtered Internet connection under strict supervision by their teacher and will therefore not have any opportunities to freely 'surf the net'.

The use of computers, iPads and the internet is an essential tool, which is used to promote and enhance all aspects of teaching and learning throughout the curriculum. To keep everyone safe we have established the following rules which must be followed when using ICT.

- ✓ I will access the C2k system with my login and password, which I will keep secret.
- ✓ I will not access other people's files without permission.
- ✓ I will only use the computers for school work and homework.
- ✓ I will not bring software or pendrives/CDs into school without permission.
- ✓ I will ask permission from a member of staff before using the Internet or printing anyting.
- ✓ I will only e-mail people I know, or my teacher has approved. (P4-P7)
- ✓ I will not open e-mails sent by someone I do not know.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not give my home address or telephone number or arrange to meet someone.
- ✓ I will report any unpleasant material or messages that make me feel uncomfortable to a my teacher
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- ✓ I understand that the school may check my computer files and may monitor the Internet sites I visit and that my parent/ carer will be contacted if a member of school staff is concerned about my e-Safety.
- ✓ I will not use Internet chat-rooms in school.
- ✓ I will never give out personal information or passwords.
- ✓ I will always remember to log-off when I am finished.
- ✓ I will take good care of the ICT resources in school and use them responsibly.
- ✓ I will not use my mobile phone in school.

Signed (Pupil)	
Date	
Signed (Parent)	

Appendix 4

Hollybank Primary School

2021-2022

Consent Form for ..... Date of Birth .....Class ……..

Dear Parent/Guardian,

This form explains the reasons why and how **Hollybank Primary School** may seek consent for various purposes throughout the year, which involves processing personal data under data protection laws.

To enable us to comply with our obligations under the General Data Protection Regulation, we are required to obtain express consent for the use of your child's personal information for processing of school data and engagement with various outside agencies e.g. School Nurse/Doctor, GL Assessment school tests or when engaging with our partner school Hollybank Primary. Without your consent we will not be able to carry out important procedures such as testing and levelling of children's work or continue with the day to day sharing of lessons with pupils from Hollybank.

FOR EXAMPLE: Hollybank Primary School uses an external body called GL Assessment for our annual testing procedures in Literacy and Numeracy. These scores provide necessary confirmation of your child's ability to the class teacher and offer direction to staff when setting future targets.

As parents/legal guardians of our pupils, all of who are under the age of 13 we ask you to complete this form on behalf of your child.

This consent form is valid for the years that your child is a pupil of Hollybank Primary School.
Consent will be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. an additional form of distributing marketing material
- Changes to school circumstances, e.g. if a new Principal reviews how the school markets itself

Consent can be withdrawn at any time by notifying the Principal and completing a new copy of this form. If you do not consent to a particular use of you/your child's personal information, you/your child will not suffer any detrimental effect as a result.

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the Principal. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Details regarding your child are kept within the secure school computer or in the school filing cabinet.

PLEASE READ THE FOLLOWING CONDITIONS THOROUGHLY AND PROVIDE YOUR CONSENT AS APPROPRIATE BY CIRCLING EITHER 'YES' OR 'NO' FOR EACH CRITERION.

If my child has a medical need I agree to their Care Plan being on display in the school staff room.	Yes/No
I consent for my child's information being shared with School nurse/doctor: Annually children are issued with the Flu Vaccine. In P1 pupils are tested for height, weight, sight and hearing etc.	Yes/No
I consent to engagement with External Support, such as the Educational Psychologist, Behaviour Support Service or the Literacy Support Service: Your child may be offered help from the EA Peripatetic Literacy Service to help improve Literacy Skills.	Yes/No
I consent to information on my child being shared with members of the School staff on a need to know basis: This will assist with children being well provided for and happy in school and in the playground.	Yes/No
I consent to engagement with Accelerated Reader programme, Mathletics & Reading Eggs: This will mean allowing the school to share data with AR such as name and age so as children's reading can be levelled.	Yes/No
I consent to engagement with and information from the Afterschool & Breakfast Clubs: This allows staff to keep you informed of what is happening in Clubs and to keep your child safe.	Yes/No
I consent to particular medical/ SEN information being shared about my child with the swimming teacher during swimming lessons.	Yes/No
I consent to particular medical/ SEN information being shared about my child with School Sports' Coaches.	Yes/No
I consent to my child's name, DOB, ethnicity, gender and info regarding free school meals to be shared with GL Assessment testing: This will allow proper processing of levels in Literacy and Numeracy.	Yes/No
I consent to my child's name being shared with the other members of the class (for Christmas cards or birthday invitations).	Yes/No
I consent to my child's name and image being used in the school prospectus, school website, See Saw, the school newsletter, school programmes and on display boards within school. From time to time images may be taken for publication in the local press, TV, social media or other promotional purposes.	Yes/No
I consent to relevant information being shared with the school mentor, from Monsktown Village Centre, if my child is chosen for this programme.	Yes/No
If my child is chosen to take part in the Boost Programme, I consent to their information being shared with Stranmillis University , anonymously.	Yes/No
I consent to my child's image being used for Monkstown's inews.	Yes/No
I consent to School Money (Eduspot) collecting my data in order to process school payments	Yes/No
I consent for my child to access the internet during school for educational purposes I understand that my child will be held accountable for their own actions and also understand that despite filtering provided by C2k, some materials on the internet may be unsuitable. I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media at home.	Yes/No

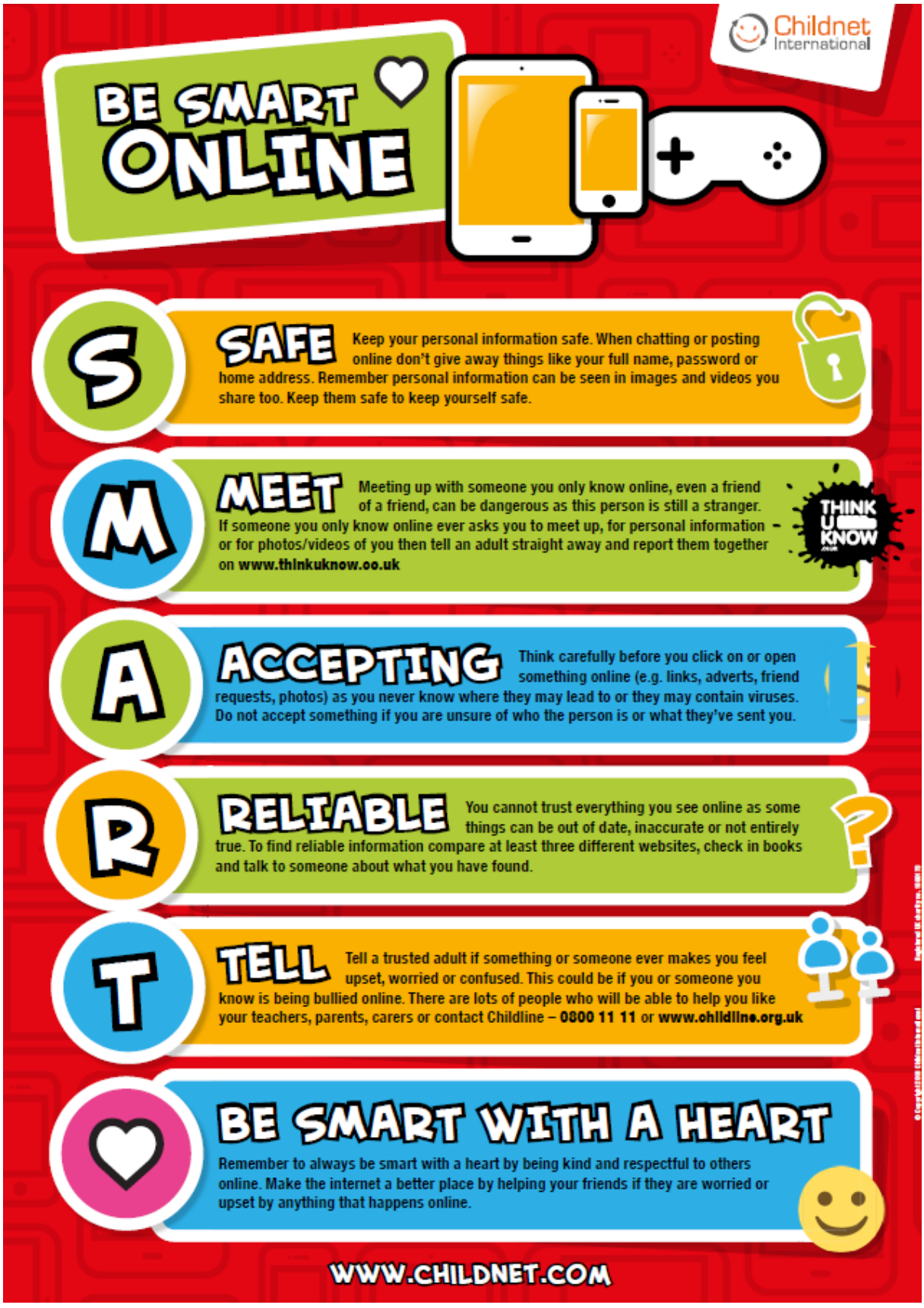
Signed by parent/legal guardian.....Print name .....

Relationship to child ..... Date .....

Should you/your child's circumstances change mid-year, it is your responsibility to notify the school and complete a new consent form.

You can grant consent to all the purposes; one of the purposes or none of the purposes. Where you do not grant consent we will not be able to use your personal data; (so for example we may not be able to let you know about forthcoming services and events); except in certain limited situations, such as where required to do so by law or to protect members of the public from serious harm. You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the School Office.
You can withdraw or change your consent at any time by contacting the School Secretary at Hollybank Primary School. Please note that all processing of your personal data will cease once you have withdrawn consent, other than where this is required by law, but this will not affect any personal data that has already been processed prior to this point.

Appendix 5


Childnet International
BE SMART ONLINE
S
SAFE
Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.
M
MEET
Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk
THINK U KNOW
A
ACCEPTING
Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.
R
RELIABLE
You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.
T
TELL
Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk
BE SMART WITH A HEART
Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.
WWW.CHILDNET.COM

Appendix 6

Smartie the Penguin

If anything happens online that makes **Smartie the Penguin** feel worried, upset or confused, he doesn't try to fix things by himself ...

Always ask an adult for help!

He stops ...

Thinks about what to do ...

And always asks an adult for help!

Childnet International | UK Safer Internet Centre | Co-financed by the European Union Connecting Europe Facility

www.childnet.com/smartie