Dear Parents / Guardians

As part of your child's curriculum and the development of ICT skills, Cumran Primary School is providing supervised use and access to a variety of digital technologies. We believe that the use of these technologies is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you and your child read the attached "Three way agreement for Safe, Effective and Acceptable Use of the Internet and Digital Technologies / ", sign and return the consent form.

Although there have been concerns about pupils having access to undesirable materials on the Internet, we are taking positive steps to deal with this risk in school. Our school network provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish.

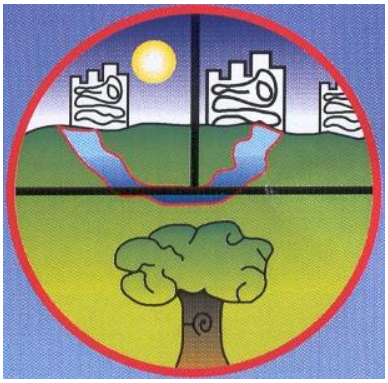
Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use or digital technologies please telephone us to arrange an appointment.

Yours sincerely,

Mrs L Smyth

Cumran Primary School



Safe, Effective and Acceptable Use of the Internet and Digital Technologies/ Online Safety Policy
2019-2021

Introduction

The statutory requirements for UICT (Using Information and Communication Technology) as a cross curricular skill states pupils need to explore (find and use information and using digital tool to investigate and problem solve), express (create and present ideas) within information technology, evaluate (review learning and process), exchange (work collaboratively online) and exhibit (showcase their work digitally); sometimes known as the 5'E's. At Cumran Primary School we use the CCEA ICT Tasks for coverage of the UICT Requirements across the 5 'E's. Assessment of ICT is ongoing and the use of the voluntary ICT Moderation enables us to assess children's UICT ability in advance of UICT assessment becoming statutory. By doing this we are developing children's ICT skills needed for life: social interactions, future learning and computer literacy for all careers.

Staff at Cumran Primary School integrates the use of the Internet, email and digital technologies daily as a teaching / learning tool to raise standards and promote achievement. Information technologies are used in the management of school information and for administration purposes.

The children in our school have been brought up in a digital age where digital technology is used for work (inside and outside of school), social and leisure activities. These invaluable resources present risks and benefits. Users must be made aware of and how to deal with the risks – online safety (short for electronic safety)

This document refers to C2k users / users, this defines pupils, non-teaching staff, teaching staff, Senior Leaders and guest users.

Who will write and review the policy?

Our Online safety policy has been developed by the school, consulting with the following documents:
EU Kids Online September 2011
Using The Mobile Phone in School Handling opportunity and risk appropriately 2010
Anti bullying Network Cyber-bullying sheet for teachers
Cyberbullying DCSF 2007
Acceptable Use of the Internet and Digital Technologies in Schools (DENI circular 2007/1)
Internet Safety (DENI circular 2011/22)
eSAFETY GUIDANCE (DENI circular 2013/25)
Effective Educational Use of Mobile Digital Devices (DENI circular 2016/26)
Online safety (DENI circular 2016/27)
It has been agreed and approved by Cumran Primary School's Online safety Committee (ICT Leaders, Senior Leadership Team, Designated Person for Child Protection, Board of Governors and Pupil Council). It has involved all stakeholders in a child's education – Online safety Committee, classroom teachers, support staff, pupils and parents. The policy will be reviewed annually and is linked to our Child Protection Policy, Safe Guarding Policy, Anti Bullying Policy, Positive Behaviour Policy and Pastoral Care policy.

Created by : ICT Leaders
Date

Approved by: Principal Date

Approved by: Chairperson of Board of Governors
Date

Approved by: Parent Representative Date

Approved by: Teacher Representative Date

Approved by: Teaching Assistant Representative
Date

Approved by: Chair of Pupil Council Date

Who is responsible for Online safety?

It is the responsibility of the Online safety Committee within our school to have a policy on the safe, healthy, acceptable and effective use of the Internet and other digital technology tools. The ICT Leaders will be the central point of contact for all safety issues within the school, ensuring that policies are current and adhered to, any breaches or abuse will involve sanctions and will be reported to the Principal and the Governors. Children and young people are born into a digital world and have grown up surrounded by information and communication technology. They may be confident at using these technologies but they may be unaware of the risks and dangers involved when doing so. All teachers who use ICT in the classroom have a duty to ensure that pupils are taught and reminded of appropriate behaviour. Online safety and anti-cyberbullying lessons will be taught to every class as part of PDMU. Head of Pastoral Care / Vice Principal Mrs. McDade encourages the prevention of cyberbullying happening and will deal with any incidents of cyberbullying that take place. Parents and carers have a key role in promoting Online safety at home. The online safety committee wish to minimise risks and through recommendations to parents / guardians support their responsibility for their children online use out-of-school. See Further Information and Advice for Parents on Online Safety section later in the policy for more advice.

The role of ICT and the benefits to learning

The Department of Education sets out plans to further the development of ICT as a teaching and learning tool, review of the emPowering School Strategy and the steps needed to ensure that the investments made in ICT are harnessed effectively.

"As new digital technologies impinge on more aspects of education, business and leisure, and their pace of change accelerates, it is important that our pupils acquire the
necessary skills and competences to use ICT effectively and confidently, as well as responsibly and safely. The use of ICT should become the norm, not just to enhance learning and teaching, but also to transform aspects of education across the whole school."
DENI Circular 2007/24

DENI believe that if the education system can maximise the use of ICT it will ensure that real added value is provided in terms of improvements in teaching and learning and in supporting the drive to raise standards for all pupils.
The ETI have emphasised the need to ensure that ICT is embedded across all aspects of teaching and learning in schools.

Developing pupils' skills in the use of ICT is a compulsory cross-curricular element of the Northern Ireland curriculum from September 2007.

Within our educational establishments we see the benefit of digital technologies to be:
Access to information, resources for staff and pupils
Access to specific knowledge from experts for staff and pupils
Exchanges between; pupils in terms of education and culture; staff in terms of support services and professional associations
Transference of data and curriculum information to other bodies e.g DENI
Approved remote technical support, management and updates of the network
Pupils to have experience and practise skills needed for life

Risks associate with using ICT

At Cumran Primary school we recognise the positive educational and social benefits offered by ICT but also recognise the dangers.
These risks include:

- Assessing or seeing inappropriate material or unwelcome content
- Spam e-mails
- Physical danger, making contact or meeting people - Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal behaviour
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device
- Sexting
- Discrimination against people
- Sharing personal information that can be given to others and used against them
- Viruses, Ad ware and Spyware
- Cyber-bullying

SBNI published January 2014 a Report 'An exploration of e-safety messages to young people, parents and practitioners in Northern Ireland'. Identifies risks defined under four categories:

Content risks: The child or young person is exposed to harmful materials.

- Contact risks: The child or young person participates in adult-initiated online activity and/or is at risk of grooming.
- Conduct risks: The child or young person is a perpetrator or subject to bullying behaviour in peer-to-peer exchange and/or is at risk of bullying, entrapment and/or blackmail.
- Commercial risks: The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs/fraud.

DENI Circular 2016/27

Users need to consider information they access and technologies they use in relation to their own safety and security.

DENI states -

Use ICT, don't abuse ICT

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.
Where deliberate misuse occurs, schools' rules and the law apply.

Who is responsible for making children aware of the rules?

As in other areas of life, when using the Internet and other technologies children are vulnerable and may expose themselves to danger (knowingly or unknowingly). It is the duty of all stakeholders involved in a child's education – Online safety Committee, classroom teachers, support staff, and parents to ensure that every child is safe and aware for the rules. The same principles should apply to the digital world as it would be applied to the physical world.

Whilst Cumran Primary School acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. All computers in the school are linked to the Internet via the C2k network which has an Internet and E-mail filtering service. C2k cannot guarantee all inappropriate material will be blocked. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people continue to be protected. Attempts to bypass filtering system or accessing inappropriate or illegal material will be reported to the school authority and or Child Exploitation and Online Protection Centre (CEOP).

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – looking for information and researching for school work
- E-mail
- Instant messaging and Voice Over Internet Protocols
- Chat Rooms and message boards / Forums
- Blogging
- Podcasting
- Wikis
- Social networking
- Video broadcasting sites – watching video clips and reading / watching new
- Webcams
- Virtual Learning Environments
- File sharing and Downloading
- Games and Gaming online
- Mobile phones with talking and texting, camera and video functionality, and Smart phones with e-mail, web functionality, listening to music, downloading and forwarding pictures and film clips, playing games and social networking
- Mobile technology (e.g. games consoles and tablets)

How will Online safety complaints be dealt with?

C2k services are monitored for all users. The school has the right to access user's files, folders and emails to monitor, review and examine the internet usage and history, communication between users and files of users this also includes the use of cloud services. This is in line with Data Protection and the Regulation of Investigatory Powers Act 2000. All user's files, folders and emails should not be regarded as private. Where necessary inappropriate items may be stopped or deleted. ICT leaders are contacted for any Online safety issue or C2k may intervene themselves. Users under investigation for inappropriate use will be disabled promptly. If staff or pupils discover unsuitable material the URL (website address), time and date must be reported to C2K Helpdesk via where possible the Principal or Vice Principal. Users are responsible for appropriate use of digital technologies. Misuse by pupils will be dealt with by a member of Senior Leadership Team. Staff misuse will be dealt with by Principal. Complaints about the Principal's misuse will be referred to Vice Principal or Chair Person of Board of Governors. Potential child protection or illegal issues will be dealt with by Designated Child Protection Officer with school authority and CEOP involved as necessary. Sanction will be linked to school Behaviour Policy. Staff and pupils will be made aware of the flowchart for responding to Online safety incidents. (Appendix A)
The school may get involved; take action or intervene in Online Safety incidents that occur outside school.

<u>How will Cyberbulling incidents be dealt with?</u>

Every incident of bullying that the staff becomes aware of will be taken seriously. When dealing with bullying behaviour the school will aim to:

1. Stop the bullying behaviour.
2. Protect and support the bullied pupil.
3. Change the attitude and behaviour of the bully.

In Cumran Primary School, the following strategies will be implemented by all staff.

4. Listen to all concerns when reported.
5. Communicate with the appropriate members of staff-

    - Class teacher
    - Head of Pastoral Care / Vice Principal Mrs. McDade.
    - Principal Mrs. Moles.

6. The teacher will record incidents as appropriate, on a Record of Concern form, identifying those involved in the bullying incident. A copy of the form will be forwarded to Mrs. McDade.

(See Anti-bullying policy for further information)

Information Security

Security of the school information system will be maintained by C2K. Virus protection performs checks and updates regularly. Portable media devices are used with permission and virus checks occur automatically on these. Internet use is monitored. Filtering / blocking of websites and email may also occur. Information and data are now stored in the Cloud. This information and data can be accessed securely from any location. Information and data need not be carried on unsecure pens and portable devices. Microsoft and Google have their own privacy policy which can be viewed at http://www.office365.co.uk/About/Privacy and https://www.google.com/policies/privacy/.

Use of the Internet

Through the Internet, school and their pupils have access to a vast up-to-date global network of information and resources. They can communicate with others (including video conferencing) and publish information. The educational value of appropriate use of information / resources and the ability to communicate and publish information on the Internet is substantial. This worldwide system of computer networks is not governed by any entity. There are also no limits or checks on the kind of information that is maintained by, and accessible to, Internet users. C2k provides the school with hardware, software and connectivity to access the Internet, which is controlled by a filtering mechanism. Use of the Internet by C2k users is monitored by C2k and incidents (bypassing filtering system, accessing inappropriate or illegal material) are reported to the Principal and school authority via C2k. The Internet filtering by C2K is based on Forcepoint Services which categorise websites for access / no access. This occurs on a daily bases therefore blocking access to newly created websites if deemed inappropriate. The filtering policy can be modified by the school's C2k manager on the Principals word to meet the demands and needs of the school in order to access more internet sites to enhance teaching and learning. There are locked down sites that can never be overwritten. The school will not have access to non-C2k internet access.

It is important to ensure that staff are regularly training in Online safety to keep up with the latest advances in the digital world. We teach our children and young people

how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through ICT and/or PDMU lessons. These lessons must be planned and provide progression and be age appropriate. Children must be made aware of the potential risks including inappropriate materials, violence and exploitation. They need to learn how to cope / deal with these risks. Pupils will understand why certain rules apply to the use of the Internet and the sanctions for improper use. Pupils will be directed to a "Three way agreement for Safe, Effective and Acceptable Use of the Internet and Digital Technologies / Online safety" that will be discussed in school and at home before they sign to show agreement of the terms.

The following concepts, skills and competencies will have been taught by the time they leave Year 7:

- Internet literacy
- Encourage children to have digital resilience.
- Use appropriate behaviour online at all times – don't say anything online you wouldn't say to a person's face in real life
- Making good judgements about websites and e-mails received (also see flowchart for responding to Online safety incidents Appendix A, A1 and A2) – child friendly version will be displayed in computer area.
- Knowledge of risks such as viruses and opening mail from a stranger
- Knowledge of copyright and plagiarism issues
- File-sharing and downloading illegal content
- Uploading information – know what is safe to upload, not to upload personal information (e.g. Real name, home/email address, mobile/landline phone numbers, friends name and details, specific interests or clubs attended) and images of themselves
- Keep passwords to yourself
- Photos, information and comments put online are available to the world, including that of others e.g. their friends, it is virtually impossible to stop the sharing of that information, photo or comment and could stay online forever. Consider their digtial footprint.
- Taught to Zip it, Block it, Flag it – the Click Clever Click Safe code / how to be SMART on the Internet KidSMART Childnet / Sid's Top Tips CEOP Thinkuknow(Appendix B, B1 and B2)
- Access to resources that outline how to be safe and responsible when using any online technologies
- Don't retaliate or reply but save evidence
- Where to go for advice and how to report abuse (CEOP – posters to advertise this must be displayed in the computer area Appendix B2) and the Childline number.

At Cumran Primary School we use a variety of resources but especially thinkuknow.co.uk and childnet.com resources for KS1 and KS2, within PDMU and ICT to teach Online safety lessons from Years 1 to 7. PSNI may also be invited into Cumran Primary School to speak to parents and pupils about Internet safety.

Location and Supervision

a) Rules for digital technology use will be displayed in computer area.

b) Internet access for pupils at Cumran Primary School is located in the classrooms and in resource areas. All such machines are in full view of people circulating in the area.

c) While using the Internet at school, pupils **should, where possible**, be supervised directly by a member of staff. Independent electronic research requires specific teacher permission and research must be conducted in designated curricular areas only. In all cases, pupils should be reminded of their responsibility to use these resources in line with the school policy on acceptable use.

d) Users will be made aware that the ICT Leaders and Principal have the ability to review files and communications to ensure that users are using the system responsibly. All uses of the Internet are logged and all sites visited by individual users are recorded. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored on school servers to be absolutely private.

At Cumran Primary School we expect good behaviour on the Internet just as we do in the classroom or school corridor. This includes materials they choose to access and language they use.

Pupils must ask permission before accessing the Internet.

Access to the Internet requires parental permission and a signed declaration by pupils agreeing to the school rules for use of the Internet. (Three way agreement for Safe, Effective and Acceptable Use of the Internet and Digital Technologies / Online safety)

The Internet is provided for pupils to conduct research and communicate with others. Planned activities should have the potential to enrich and extend learning. While the use of information and communication technologies is a required aspect of the statutory Northern Ireland Curriculum, access to the Internet remains **a privilege and not a right**. It is given to pupils who act in a considerate and responsible manner, and should be withdrawn if they fail to maintain acceptable standards of use. Use of the computer system without permission or for inappropriate purposes could constitute a criminal offence under the computer Misuse Act 1990.

During school hours or for home learning activities that require Internet access the teachers will guide pupils towards appropriate materials. Outside school hours families bear responsibility for such guidance – just as they exercise control with information sources such as television, telephones, movies, radio, and other potentially offensive media they must do the same with the Internet.

Cyberbullying

Cyberbullying is when technology is used to bully. The Internet can also be used to help those who are bullied. With changes to technology we see the development of new ways in which to bully, slander and abuse. The bully can bully anonymously or from an unknown location. The audience can be very large and reached rapidly. The victim can be attacked 24 hours a day, 7 days a week etc with no place, not even their bedroom a safe haven.
All pupils need to consider their conduct online. It could be the case where cyberbullying may be unintentional.
All stakeholders in children's education are responsible for preparing children within Cumran Primary School for the threat of cyberbullying, educating them to deal with that situation and to encourage them not to be a cyberbully.

Using The Internet

Staff and pupils access the internet via C2k Education Network requiring an authentic C2k username and password providing internet filtering that is auditable and reports are available to the Principal. Inappropriate use of the internet will result in removal of access. Our school does offer protection with the supervision of children and a filtering software system is installed but this software is not always fool proof. Neither the school nor C2k can accept liability for materials accessed or any consequence of Internet access. Adult supervision of children's ICT use is preferable; it is not always realistic or practical outside school. We must therefore alert children to the risks they might encounter and help them to develop a safe, healthy, acceptable and effective use of the Internet which can be used in any setting – school or home. Children must be empowered with the knowledge of how to deal with situations they may encounter. (Also see flow chart for reporting Online safety incidents – Appendix A, A1 and A2).
When registering on a website in school or for school purposes, school details such as address, email address and phone numbers must be used. Not staff or pupils' personal information. Access to websites should enhance the pupil's learning experience.

Pupils using search engines are expected not to deliberately seek out offensive materials. Should any pupil encounter such material accidentally, they should report it immediately to a teacher.
When using the Internet at Cumran Primary School, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws. Children must be aware that plenty of the material available on the Internet is correct information however there is also incorrect information. Children need to consider the author of the material, date it was created and the content. Like books information from the Internet must not be plagiarised. With such vast amounts of information available on the Internet search tools provide the opportunity to locate specific information quickly and easily. The search results will turn up a huge number of sites containing the keyword information. Children must make sensible keyword choices, omitted words such as 'of' and 'the' and check to see if results are displayed in rank order of priority. Some search engines have a filtering facility which may remove unsuitable sites.

Using Email

Email is a means of communication, messages can be sent over the Internet to anywhere or anyone in the world. Text, images, pictures, sound, animations or movies can be attached to an email. Like any business schools see email as a valuable tool for the communication of information, in Cumran Primary School staff use it daily. Email is now an essential part of most people's lives. The school info@ mail account is managed by the Office Assistant and the Principal to ensure incoming mail is addressed and forwards to the relevant staff members as required.
Email has the potential to help with literacy skills – spelling accuracy (emails will not send if address is spelt incorrectly), language succinctness (emails should be brief and clear) presentation (typed text- clear to read) and another means of communication other than verbal. We encourage the use of email for communication between colleagues in schools and industry, between pupils and teachers, between pupils and pupils. Emails sent to external organisations must be carefully written and authorised before sending in the same way as a letter on school headed paper. Staff are encouraged to use C2k email system for school based business and not use home emails accounts. The C2k Education network provides security and protection to email accounts scanning all school emails both incoming and outgoing for viruses, malware, spam and inappropriate content.
Messages will be analyses by C2k. Email considered inappropriate will be held and only released once content is checked. Messages may be held because of spam / oversized attachments / racial, sexual and profanity terms used / encrypted mail / inappropriate images / executables and banned file types.
Despite an email filtering system, unwanted emails (spam / spoofing emails) may still get through. These unwanted emails may contain inappropriate content which is

received or sent to the user's entire address book, they may be hiding a virus or obtain sensitive information from a user's account. Other terms linked to this include phishing and pharming – tricking people into revealing information / data. Other types of unwanted emails include:

- Angry / abusive emails– sometimes called flaming
- Bullying / harassment emails
- Blackmail emails
- Bombing emails– a large message or number of messages that causes the user's email program to crash

Email as a form of communication continues to grow in popularity, we must make children aware of the unpleasant side to emails mentioned above and prepare them to deal with emails effectively to protect the school's network against viruses. In Cumran Primary School children will be taught the appropriate tone and language to use. Children will be made aware that they need to think and evaluate the source of emails and attachments. If they receive abusive or bullying messages, they need to seek help from an adult (teacher, parent or carer) and they must not respond to the message. Any information they find or receive that has content or contact that makes them feel uncomfortable should be reported to an adult immediately. Spam or junk messages should not be opened, responded to and should be deleted. Personal information must be kept private.

Some webmail providers allow email addresses to be shared with third parties. Many offer effective email filtering tools which many be optional setting that needs selected, therefore pupils are not permitted to use any other e-mail service in school except the one provided by C2k. All our pupils in year 5, 6 and 7 have an email address created by C2k. E.g aperson123@c2kni.net. The ICT Leaders can choose to activate or deactivate pupils email accounts.

Password Protocol

All users are responsible for the secure use of their C2k user name and password. All children in Cumran Primary School will be allocated a user name by C2k. Pupils will login with their C2k username (e.g. aperson123). Pupils in year 1 – 4 will be given a simple password created by the ICT Leaders or class teachers. Pupils in year 5 will set their own password. In this instance, the teacher will make a note of each child's password. The ICT Leaders will also keep a copy of this document, as system administrator. Pupils in year 6 and 7 must take responsibility for their own password, which is secret. Pupils will use only their own network login and password. Passwords must be 8 characters long and not related to their name or a sequence of numbers. Pupils will be discouraged from using look alike letters e.g "a" replaced with "@" and "s" replaced with "$". If passwords are written down they must be kept safe.

Using Instant messaging (IM) and Voice Over Internet Protocols (VoIP)

IM is a means of communicating with people in real time with people on a pre-selected friend/buddy list. Users normally have to download an application to your device or register by creating a username and password to a web-based service which does not need installing. Programmes let you see which of your list of contacts that are online when you are. IM is generally more private than publicly open chat rooms.
VOIP programmes offer unlimited free phone calls anywhere in the world using an Internet connected devise. Calls can only take place between people who have downloaded the same application.

Users typically use IM as an extension to their regular social lives to talk to friends outside of school or work. It is a quick and effective way to keep in touch. It can be used for collaborative work and research. Some IM products a hold up to 600 contacts, some users may see having as many 'friends' as possible important but will only know a small proportion of the contacts on their list.

Using Chatrooms and Message Boards / Forums

There are many chat sites online. Typically, chatrooms are thematically organised around interest, age or location. Chatrooms allow groups of people form access the world to hold text (and sometimes voice) conversations in real time.
To contribute to a discussion users, type a message into the message box, the message is displayed for all to see on the screen and so the discussion continues. Chat rooms can offer private chat rooms for users where other users cannot see the conversation – this is known as whispering. This is similar to instant messaging which is an online chat that is private between two people. The conversations cannot be moderated or joined by other people. Before you can chat with anyone invites and agreements need to be completed. With this form of communication people are using fake or pseudonym (acceptable and encouraged practises in chat rooms) and are not dealing face to face with people. They are free from real world stereotypes such as age, race and appearance. For young people this can be an easy way to meet new people or explore issues which they are too shy to talk about in person.

Message boards allow different people to add replies to discussion topics creating chains of replies around particular topics which may take place over several months. Some message boards are moderated – no new messages will be published publicly until the owner reviews them but many others are monitored only by users who are expected to report any inappropriate messages.

Online chats have the potential for enhancing learning for pupils. Pupils would be able to join chats hosted by important figures (television personalities, business people) or their peers in real time anywhere in the world about themed or topic related discussions and exchange ideas. Since many people can join chatrooms, they are very useful for sharing information, experiences, comparison of lifestyles or collaborative working.

Public chatrooms and message boards can be populated by anyone since accounts usually require an email address to verify a user's identify. It therefore has the potential for exploitation; users may pretend to be someone else. People can behave inappropriately of abusively. Chat rooms also provide the opportunity for some users to use and invent acronyms to keep conversations private and to exclude other users creating the opportunity for bullying to develop. Nasty or threatening messages can be sent without the target necessarily knowing who they are from. Groups may ostracise and ignore individual children. Young people may be persuaded to give out private information or enter an apparent friendship with people who are lying to them. 'Grooming' of children may occur – a paedophile could develop a relationship with a child anonymously under the guise of a peer who is the same age etc. Chatrooms do not tend to carry age verification therefore children can visit chatrooms of an adult nature.

Children working at level 4 or 5 of the new ICT curriculum pupils are expected to share ideas and communicate with pupils in another school. In school this will be done through Fronter and Lync a safe, secure and well policed environment. Children will be supervised when involved in these prearrange chats with other schools. Information is available to parents about these new technologies and how best to deal with instant messaging and chat rooms at home at the end of this policy.

<u>Using social software</u>

Blogs and weblogs are one of the first and most well known social software. These social media tools provide the opportunity for an online diary or journal. Other tools are now available such as:
Moblogs – blogs sent from a mobile phone
Wikis – collaborative web pages that can be modified
Podcasting – audio broadcasts that are available over the web

Social networking is the term that describes online communities where content such as text, photos, music and video is created and shared. Users can create profiles, list interests and other details, post comments, exchange instant messages and develop a list of friends and easily stay in contact. They are used to socialise with friends and other people online, express themselves and meet up in much the same way as they

might do at a social event. These websites offer public and private spaces and let users express themselves creatively by selecting and creating content. Users can set controls and permissions over who can access their profiles and pages. Young people can spend a lot of time on the look and content of their pages. They may contain personal information about themselves and their friends. Children can mistakenly view publicly available sites for private and personal places posting photos for their friends which may be inappropriate or embarrassing in other contexts. Children must be aware of nasty comments posted by them or about them. People might use their own sites to spread rumours or make unpleasant comments about others or post humiliating images or videos. Fake profiles are common and these might be used to pretend to be someone else in order to bully, harass or get them into trouble. Unfortunately, cyber bullying and grooming can take place through social network sites. C2K block access within school to social networking sites. Many of these sites require children to be over the age of 12 before they can register. Many parents allow children to register on these sites and agree to the terms and conditions which may not have been read by either party in detail. We at Cumran Primary School encourage parents and carers to read the terms and conditions along with their child. This will provide opportunity for discussion about Online safety issues. We would recommend that children and parents adhere to age restrictions on membership of social networking sites and ensure privacy settings are activated and access to profiles is password protected. Using the website www.thinkuknow.co.uk children will be taught to keep personal information or personal details which may identify their location private and protect the information of others. Pupils will be advised not to place personal photos on social networking sites. They will be made aware that information presented is available to the public and they should consider information they present carefully. Pupils should deny access to unknown users only accepting or inviting known friends.

Using Video Broadcasting Sites

Video broadcasting sites are a place online where clips are uploaded and shared. Popular clips can be seen by hundreds of thousands of visitors to the site who may rate and post comments. Video footage can also be embedded in other sites and pages that link to video-hosting sites. Content on these sites can provide entertainment, useful resources including educational resources. Children need to be made aware that they may access inappropriate material such as violence and pornography. Children need to be wary of uploading any content, it could make them contactable / vulnerable or might lead to embarrassment of themselves or others.

Using Webcams and Teaching in a Virtual Classroom

Webcams are small digital cameras used to record photographs or videos which can then be posted or forwarded. They are most commonly used to see someone that you are talking to online in real time. They can bring far off places to life, view experiments used for video conferencing and to facilitate collaboration between schools in different parts of the world and allows families stay in touch. With the use of a web cam and Collaborate software the Virtual Classroom service enables all schools to use video conferencing to collaborate with others both locally and internationally. Children can interview experts, meet important figures and be taught by other individuals with an educational focus in mind. Guests and teachers must agree to protocols before a session occurs. Parents and Carers should agree for their child to take part in video conferencing. Children should be made aware of the protocols for video conferencing (Appendix C). Teachers and staff can attend staff meetings and training sessions delivered by other individuals. These guests who are invited to attend a conference can only be invited by teachers who set up a meeting for a given time. Access to the conference is through an email. Webcam will be switched off at all times except during conferences. The teacher will always be present during conferences. Teachers and staff will initiate, make or answer a video conferencing call. Outside of school children can be persuaded to take or send inappropriate photos of themselves. Once someone else has content the children would not like their parent to know about or be made public they are at risk of being further manipulated or threatened. Webcam use can be difficult to supervise if the computer is in the child's bedroom or private space. It is rare but there have been cases of people using virus programmes that can hijack the output of a remote webcam and send the images to their own computer.

Using Virtual Learning Environment - Fronter

Fronter is a learning management system or virtual learning environment (VLE) which supports online learning for the entire Northern Ireland education system. It supports collaboration in the learning process through public and private rooms, discussion areas, access to email and work areas. Children and teachers can access a library of resources: educational information, pictures, videos, games, quizzes, votes, links to useful websites and news reports. Fronter's virtual learning environment has many features designed to enrich the learning experience for school children. Teachers can set up rooms or a bank of materials for their pupils to use and access. Pupils can track their progress in an online environment, read messages from their teacher. Parents are responsible for their children's out-of-school online use of Fronter. Pupils will be expected to use appropriate behaviour when using Fronter and adhear to the school's Acceptable Use Policy (Three way agreement). Access to Fronter is only through authenticated access using user names allocated by C2k. The technical managers in school can choose to activate or deactivate user's access. Hacking can provide a range of opportunities for cyberbullying – including sending

nasty messages, posting inappropriate comments and deleting work from someone's account. Pupils should be aware of this and as recommended in the school's AUP pupils should not share their password with others.

Using File sharing services or peer-to-peer networking (P2P) and downloading

File sharing is allowing others, whom you may not know, to access information on your computer via the internet, it allows users to share files, computing capabilities, networks, bandwidth and storage including music, films, images, software, videos, games, documents and personal files. P2P is a popular method of exchanging music, film or TV files directly form one or more computers to another without it passing through a central point. Some file sharing software is free but others charge to download or share files. The use of file sharing software is recreational and unlikely to be used in schools however children must be educated about the issue associate with it. Files available for downloading may be made available illegally. Using illegal file-sharing programmed exposes users to the risk of unwelcome content such as viruses, pornography and violent images. File-sharing software can also compromise privacy and security by opening up the computer and sharing what's stored on it with the outside world. Copyright law applies to downloading, sharing and streaming just as it does with CDs and DVDs. If content is made available to others or content is downloaded from an illegal site then a law has been broken and there may be serious penalties. There are sites such as iTunes and Napster that allow you to download files without breaching copyright laws as a fee is paid to download.

Games and Gaming Online

Computer games are popular with children. Most of these games are played online. They are accessed through online gaming sites, where chat between players across the world is facilitated or on consoles and other devices such as mobile phones and computers which use a wireless connection to enable people to play against each other or message one another. In virtual world gaming - 2 or 3D online sites where users design their own avatars, explore and create their own environments are also popular. Gaming has been shown to help develop many positive skills such as leadership, decision-making, problem-solving, teamwork and collaboration. Physical games can provide children with a fun way to exercise. Pupils and parents should be aware that many games are designed for the adults and are inappropriate for children containing adult themes and explicit imagery. Games carry labels which indicate the age they are appropriate for. Games and virtual worlds accessed online will be harder to monitor for appropriateness of content. Completing levels and finishing games are addictive and children and parents should consider the length of time spent on games. Pupils need to consider their behaviour during online gaming - they may get so involved that it brings the risk of name-calling, nasty comments and abusive or

derogatory remarks. Children should also be reminded that it leaves them open to contact from someone who may wish to bully, abuse or groom them. Players can pick on weaker or less experience players repeatedly killing their character, this is known as 'griefing'.

Using Mobile Digital Devices (Mobile phones / Smart phones and Tablets)

Smart phones are becoming increasingly popular amongst children. The range of services that phones provide is also increasing. Making calls, sending and receiving texts SMS or Short Message Service allow users to send and receive text messages, MMS or Multimedia Message Service (text, sound, images and video) and telling the time. Phones now have enhanced features capable of a range of functions such as: making calls over the mobile provider networks or via the internet using applications (VoIP) e.g. iMessage, Skype or WhatsApp, browsing the internet, taking digital images and videos, listening to music, playing games, social networking, watching videos and TV (entertainment services - video streaming, TV downloads, downloadable video clips from films and sporting events, music, horoscopes and games), checking emails, video messaging, and location based services (maps and route planners). You can personalise your phone by downloading 'apps' which carry out fun and useful functions, from checking train times to caring for a virtual pet.
A mobile phone is a powerful and important tool that offers freedom, independence, a source of mobile entertainment, for storing files, taking notes, capturing evidence and research via an internet connection, a way of communicating with friends and making contact or being contacted. They can be used in emergency situations and emergency services can use it as a location finder. Supervision of a young person's use of their mobile phone is far harder than monitoring their use of the family computer. Mobile phones are potentially always on and rarely shared. The risks associated with mobile phones are:
Children can create and circulate content (including inappropriate content) with ease once forwarded content is almost impossible to control and can easily spread by passing on.
Access and exposure to inappropriate materials (images and videos) – pornography, violence, dangerous or illegal activities. Material may be age-inappropriate, inaccurate or misleading.
Physical danger – making inappropriate friends (including grooming by adults) and meeting them, photographs taken and posted on websites without knowledge or permission and location finder capabilities misused (pinpointing the exact location of a child).
Cyberbullying – making nasty calls or sending nasty text messages, taking and sharing humiliating images and videos, capturing and sharing acts of bullying. Content can be posted online or sent from phone to phone. Attacks can happen day or night, in school or outside school making it difficult to escape or ignore.

Legal, financial or commercial issues – doing something that breaches another person's rights, or breaking plagiarism and copyright laws (in relation to downloading music or games), easy access to chargeable content in the form of music, images, videos, games, downloads, ring tones, logos and other services.
As mobiles are personal devices, they are hard for parents to monitor and supervise access. Children therefore need to be taught that as with all new technologies general Online safety recommendations apply. In Cumran Primary School, children will be taught the appropriate conduct for using mobile phones. Children will be made aware that they need to think and evaluate the source of information. If they receive abusive or bullying messages to seek help from an adult (teacher, parent or carer) and they must not respond to the message. Any information they find or receive that has content or contact that makes them feel uncomfortable should be reported to an adult immediately. Spam or junk messages should not be opened, responded to and should be deleted. Personal information must be kept private. Pupils will be encouraged to never share images and videos of themselves. Parents should encourage children to obtain permission and make them aware of the cost implications for calling a premium rate service / numbers.

The staff recognise the potential difficulties that may arise with inappropriate use of mobile phones by pupils. We would strongly discourage children from bringing mobile phones into school, however, if a parent or guardian feels that a mobile is essential for journeys to and from school, we would ask for permission to be granted from the Principal or the Designated Teacher for Child Protection.
Staff, volunteers, and visitors must be made aware of the dangers associated with the use of mobile phones in close proximity to pupils and therefore should not be used in front of them during the school day. With mobile access to the Internet and their ability to record pictures and sound, an innocent action could be misinterpreted by a pupil. Staff must also consider location, as the use of a mobile phone at the swimming pool, on residentials, or when pupils change for PE is in appropriate. It is assumed that staff recognise how inappropriate it is to use a mobile phone in class. Mobile phones should therefore be switched off during class times.
Signs are displayed in the school entrance area to ask all staff and visitors to the school to ensure mobile phones are switched off and not in use during the school day.
Tables have the ability enhance teaching and transform learning if used correctly. Photos, audio, video and text can be captured and collated to create and construct a personal piece of work e.g. images, video, podcast, blogs and presentations etc. We do not recommend them for researching due to slightly less strict filtering the wireless access provided. The mobile nature of tablets makes them good for catching a moment of learning that can be reflected and review by the pupils and the teacher e.g. audio, photo and video of work used on a plenary session shown on the IWB to create a discussion. Shared work can be peer and self assessed. They provide the opportunity for the children to record the verbalised thinking process. Pupils learning, announcements and events that have happened in school can be shared

and made accessible to parent through for example Seesaw. (Please see AUP for the use of Seesaw for more information).

School Website and Exhibition of Content

There are occasions when photographs, videos and children's work may be showcased to record and exhibit school activities or to publicise achievements. Photographs, children's work and / or video footage may be published in newspapers, television programmes, school / education and library board / educational publication, video hosting websites, 3rd party school partnerships e.g. Nerve and Capita, school intranet / Internet / website and social media. Pupil's full names will not be used on the website particularly in association with photographs. On occasions 3rd parties may use photographs and videos of pupils on their websites taken during events / activities that have been carried out at the school with pupils, no pupil names will be used. Parents are asked for permission for the use of photographs (see Appendix D).

Guest Users

Parents and members of the community may use computer facilities within the school. They will be allocated a user name and password for use in that session. This will provide access to the Internet and software available on the school network. They will not be able to save work onto the school network or access any school documents. Anyone using the school's computers will be required to sign an acceptable use policy.

Staff Users

Downloads used in school

Any resources or materials downloaded outside of the C2k filtering should be suitable for use in the classroom.

C2k Network

No 3rd party switches or devices can be connected on the C2k network. No servers or services or user access can be installed or provided on the C2k network. All 3rd party software installed on devices on the C2k network should have the appropriate licence and be secure. The school must ensure the Comms Cabinet is not used or altered by a 3rd party. All power and cabling is tested and certified.

C2k Users

Only current staff and students will be available for use. Leaving dates for staff and students will be entered promptly in SIMS. Fictitious usernames will not be created for staff or pupils. User names will only be used by one person. Users with nominated roles must be kept up to date. SLT are aware of the role of the C2k Manager (see C2k exchange EN072 sheet for further details) and the areas of responsibility delegated to other staff.

Nominated Roles
SLT is aware of the role of C2k managers and area of responsibility delegate to other staff. Nominated user's roles are kept up-to-date via form on the c2k Exchange.

Insurance and Care of C2k and school's own equipment
The school with take precautions to secure C2k's and school's own equipment at the end of each school day. C2k portable devices are only insured while inside school and alternative cover must be provided if taken from the school by staff. C2k and school devices must be used for school work only.

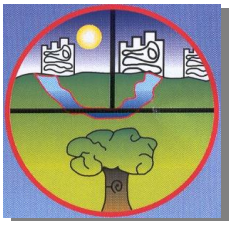
Policy Review

This policy will be kept under constant review. It will be modified if necessary to meet changes in the curriculum. The over all ICT programme for the school will be evaluated at staff meetings, both formal and informal, and if problems are identified appropriate action will be taken.

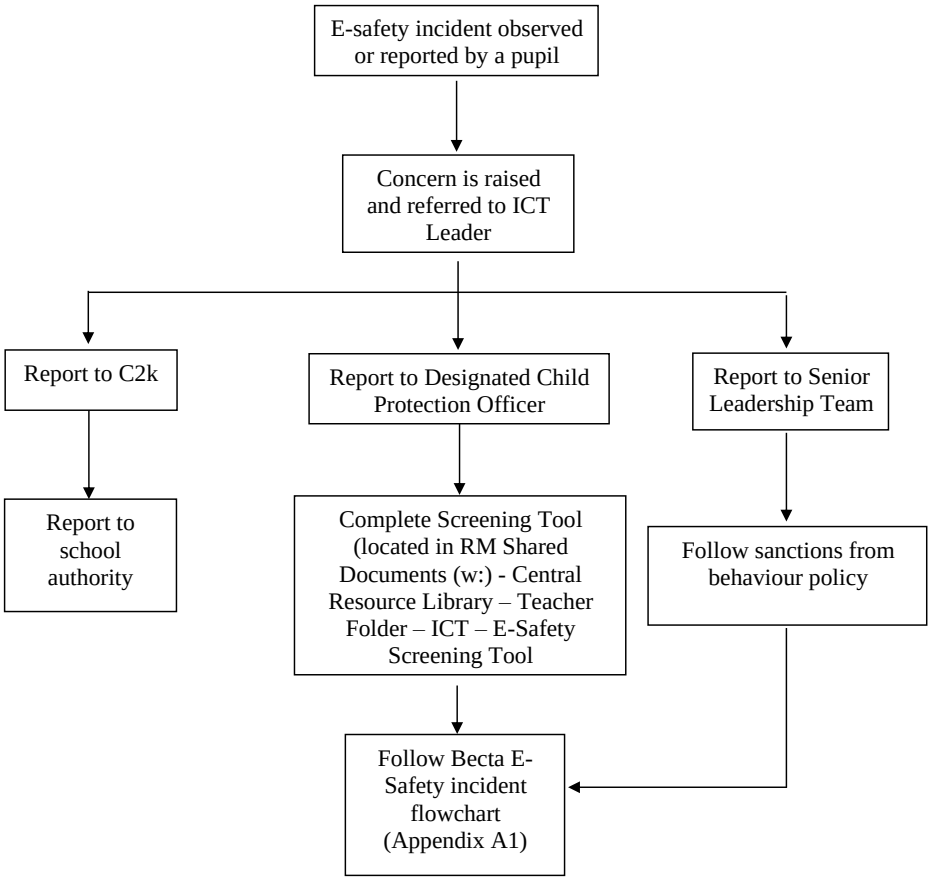
To be reviewed: 2021

Appendix A

Cumran Primary Staff and Teachers' responding to incidents



School flowchart for Online safety

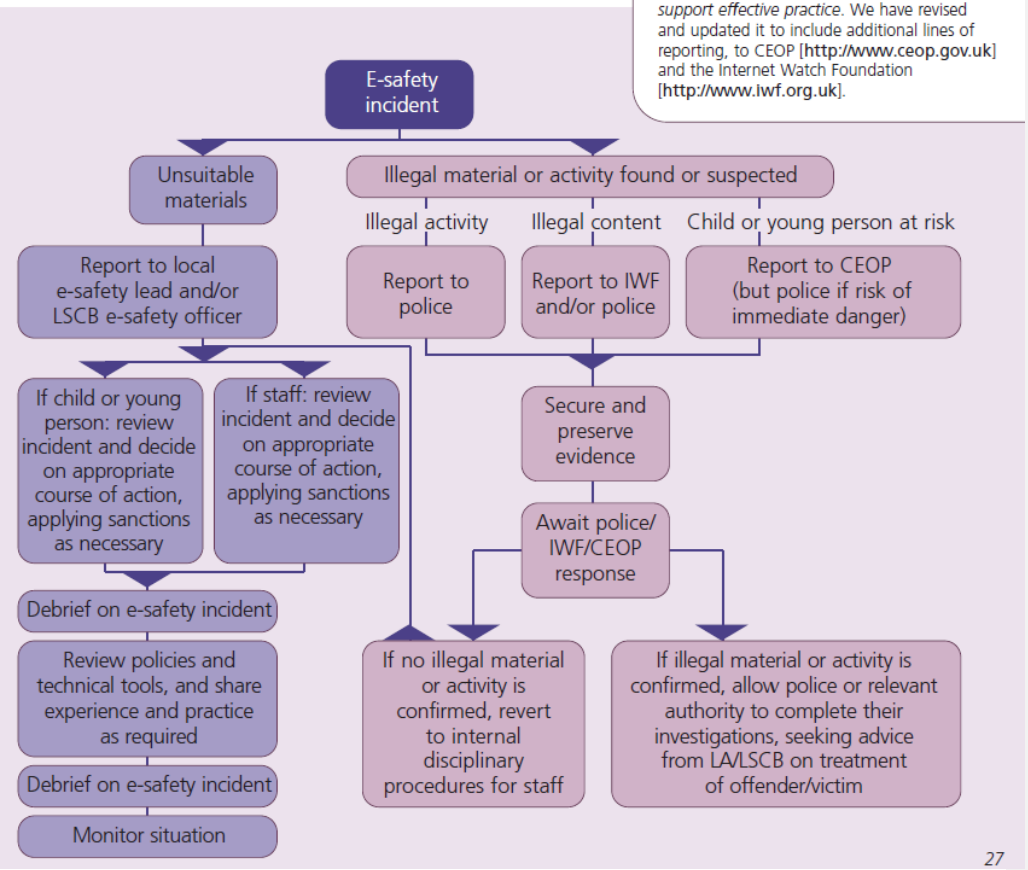


Appendix A1

Becta

flowchart for responding to e-safety incidents

Note: this flowchart originally appeared as 'Flowchart for responding to internet safety incidents in school' in the Becta publication *E-safety: Developing whole-school policies to support effective practice*. We have revised and updated it to include additional lines of reporting, to CEOP [http://www.ceop.gov.uk] and the Internet Watch Foundation [http://www.iwf.org.uk].



27

The Online safety flowchart below for responding to incidents comes from the following Becta Booklet:

Safeguarding children online: a guide for local authorities and local safeguarding children boards

Published: 19 March 2007

Publication ID: BEC1-15472

Appendix A2

Cumran Primary School

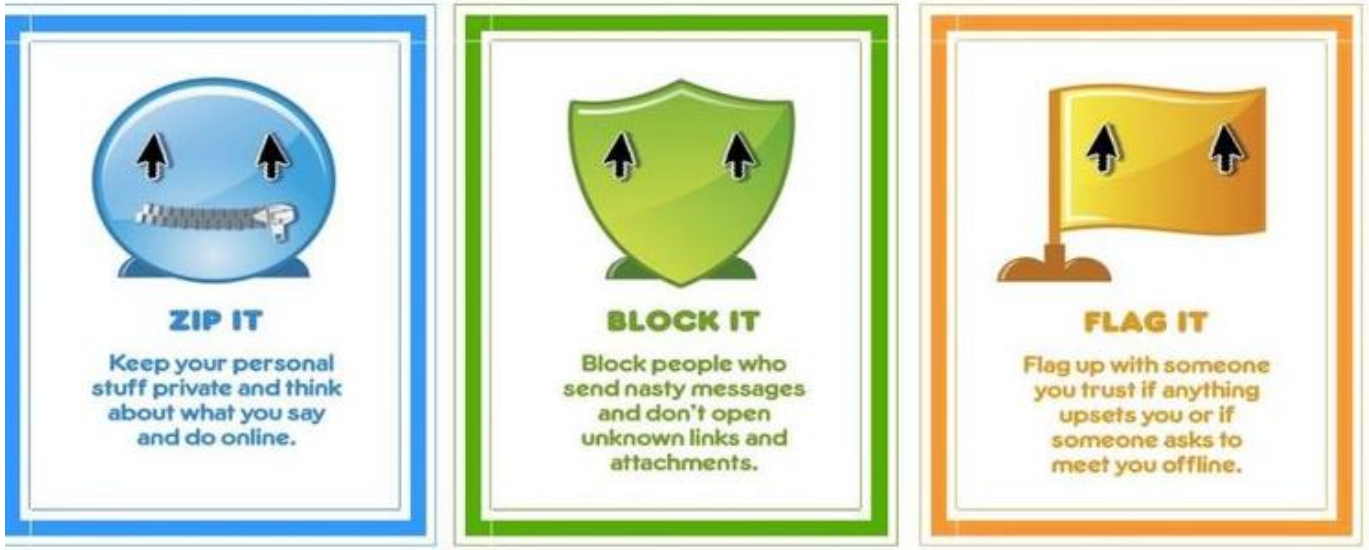
Pupils' flowchart for responding to Online safety incidents

I don't like what I can see or hear on the computer

Switch off monitor, close laptop lid or put table screen to tablet screen to lock / sleep

Tell a teacher

Follow the code to stay safe online



Click Clever, Click Safe!

Appendix B

Appendix B1

Childnet International
www.childnet.com
Be Smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.
ZIP IT
m
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.
a
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
BLOCK IT
r
RELIABLE
Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.
t
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk
THINK U KNOW
FLAG IT
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Appendix B2

SID's Top Tips
THINK U KNOW CO.UK
Top Tip Number 1
People you don't know are strangers. They're not always who they say they are.
Top Tip Number 2
Be nice to people on the computer like you would in the playground.
Top Tip Number 3
Keep your personal information private.
Top Tip Number 4
If you ever get that 'uh oh' feeling, you should tell a grown-up you trust.
CEOP
A Child Exploitation and Online Protection Centre Education Initiative
ChildLine 0800 1111
The project is co-funded by the European Union, through the safer Internet Plus programme http://ec.europa.eu/saferinternet
check out our site – www.thinkuknow.co.uk

Appendix C

Cumran Primary School

Protocol for using Video Conferencing

All participants must agree to protocols before a session occurs.
This can be agreed by email or in writing.

- A trail should be carried out beforehand to prove link quality
- Webcam will be switched off at all times except during conferences
- External participant to the C2K system should have a CRB check or countries equivalent
- Guests who are invited to attend a conference can only be invited by teachers who set up a meeting for a given time
- Video conferences must have an educational purpose
- Teachers and staff will initiate, make or answer a video conferencing call
- The teacher will always be present during conferences
- All partakers must be known and public (whether they contribute or not) – no private or hidden observers (either on line or in broadcast areas)
- All participants must be made aware of and agree to recordings of the session
- Parents and carers should agree for their child to take part in video conferencing
- Children to know and follow agreed rules
- Children must also follow class rules
- All parties have the right to use or not use video
- All partakers should maintain acceptable standards of manners, behaviour and language throughout
- Parties can leave the session at any time
- Lesson/training objectives to be made clear at the start of or before a session
- Minimum disruption – eg. Stay in room throughout whole session, Make sure toileted before lesson
- Listen to whoever is speaking / Take turns to speak / Respect what others say

Further Information and Advice for Parents on Online Safety

Recommended websites with resources available to Parents and Carers are detailed below. These resources make you aware of what your child/ren are doing online and the risks associate with this. They provide advice on Tech Tools such as filters, password and pin protection and safe searching. The resources provide guidance on how to talk to your child, developing rules and restrictions and how best to supervise. Using these resources you will understand how to communicate positively and build your child/ren's trust.

Think U Know
https://www.thinkuknow.co.uk/parents/

Child Net International
http://www.childnet.com/parents-and-carers

UK Safer Internet Centre
http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers

NSPCC Online Safety
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Net Aware
https://www.net-aware.org.uk

Internet Matters
https://www.internetmatters.org

Be Share Aware
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/

Get Safe Online
https://www.getsafeonline.org/safeguarding-children/

Webwise
http://www.webwise.ie/parents/advice-top-10-tips-for-parents/

BBC
http://www.bbc.co.uk/webwise/0/21259413

Safe Guarding NI
http://www.safeguardingni.org/parents-and-carers

UK Council for Child Internet Safety
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

In addition to the recommended resources and websites and in the "Safe, Effective and Acceptable Use of the Internet and Digital Technologies / Online safety Policy" parents are given the following guidance by Cumran Primary School:

- A home computer with Internet access should be situated in a location where parents can monitor access to Internet.
- Parents should agree with their children suitable days/times for accessing the Internet.
- Parents should be aware that downloading needs to be carefully considered.
- Parents should discuss with their children the school rules for using Digital Technologies and implement these at home. Parents and children should decide together when, how long, and what comprises appropriate use;
- Parents should get to know the sites their children visit, games their children play, and talk to them about what they are doing;
- Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials.
- It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;
- Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.
- Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such

messages or images. If the message comes from an Internet service connection provided by the school, they should immediately inform the school.

How to report abuse or seek help and advice

This is information for adults that should be shared with children

Reporting suspicious behaviour online with or towards a child –
Contact – CEOP (Child Exploitation and Online Protection)
A virtual taskforce where you can report any inappropriate or potentially illegal activity towards a child online. E.g. an online conversation with someone who a child thinks may be an adult, who is treating a child in a way which makes them feel uncomfortable, or who is trying to meet a child. If a child is in immediate danger contact 999 for immediate police assistance.
How – http://www.ceop.gov.uk

Reporting illegal content online
Contact – The Internet Watch Foundation
The UK's hotline for reporting illegal content hosted worldwide and content that is criminally obscene and or an incitement to racial hatred hosted in the UK.
How – https://www.iwf.org.uk

Help and advice for adults concerned with their own or someone else's behaviour, including that of young people
Contact – Stop it Now!
Confidential advice and support to adults that might be unsure or worried about their own thoughts or behaviour towards children, or the behaviour of someone they know, whether they are an adult or a child.
How – http://www.stopitnow.org.uk or 0808 1000 900

Help and advice for victims of Cyberbullying and those who support them
Contact - Kidscape
A UK charity committed to keeping children safe, established specifically to prevent bullying and child sexual abuse. The charity works with children and young people, their parents and carers, to help equip vulnerable children with practical non-threatening knowledge and skills in how to keep themselves safe and reduce the likelihood of future harm. Kidscape also offer a range of training programmes for both children and those who work with them.
How – http://www.kidscape.org.uk

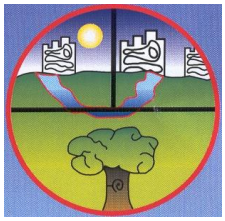
Premium rate services on mobile phones
Contact - PhonepayPlus
The industry regulator for phone-paid services. It investigates complaints, fine companies and bar access to services that do not comply with the published PhonepayPlus Code of Practice.
How - http://www.phonepayplus.org.uk

If children and young people receive nuisance calls or are bullied by mobile phone, they should contact their mobile operator for further information and advice.

General help and advice for children and young people
Contact - NSPCC helpline
If you're worried about a child, even if you're unsure, contact our professional counsellors 24/7 for help, advice and support.
How - https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/ or help@nspcc.org.uk. or 0808 800 5000

Contact – Childline
Childline is a free and confidential helpline that is open 24 hours a day to talk about any problems
How – http://www.childline.org.uk or 0800 1111

Cumran Primary School



Three way agreement for Safe, Effective and Acceptable Use of the Internet and Digital Technologies / Online safety

Pupils

The school computers, laptops and tablets have Internet access to help our learning. The internet can be a great place but we must remember there are people out there who may wish to take advantage, abuse, scare or bully us online. These rules help us to be fair to others and keep everyone safe.

General Rules

- I am responsible for my own behaviour on the computer, laptop and tablet just as I am anywhere else in school. I will follow my class charter and the school rights respecting actions.
- I will respect the hardware and software that is available to me.
- I will respect the work of others.
- I will use only my own network login and password, which is secret.
- I will only use computers, laptops and tablets for schoolwork and home learning unless permission has been granted.
- Personal printing is not allowed on our network for cost reasons.
- I will use a password that is 8 characters long and isn't related to my name or a sequence of numbers (year 5 – year 7).
- I understand that I must never give out my name, home address or phone number, school name, address or phone number, or email address, or arrange to meet someone.
- I understand that I must not give my friends' personal information or bank or credit card details.
- I will only look at or delete my own files.
- I will not access other people's files unless permission has been given.
- I will not bring in media or disks from home or outside school for use in school.
- I will not use storage devices unless permission has been given.
- I understand that the school has the right to access my file, folder and mail if necessary
- I will not play computer games or apps unless specifically assigned by the teacher.
- I will get the teacher, parent or carer to check the content if I create my own website.
- If I need help I know who to ask.
- If I see anything on the Internet, in a message or in an e-mail that makes me uncomfortable, unhappy or something I do not like, I will tell a teacher or a safe adult immediately.
- I know that I can go to www.thinkuknow.co.uk for help.
- I know that I can contact the Police on 101 or contact Childline on 0800 1111 if I am uncomfortable or worried.

Internet use

- I will ask permission from my teacher before using the Internet and will only access those services I have been given permission to use.

- I will use the Internet to help me learn and I will learn how to use the Internet safely and responsibly.
- I will not deliberately seek out offensive materials. Should any appear accidently I will report it to a teacher immediately.
- I understand that the school may check my computer files and the Internet sites I visit.
- I will never post photographs or video clips without permission and never include names with photographs.
- I will not copy text, images, sounds, animation, videos or music that breaks copyright laws.
- I will not sign up for any services or buy any goods.

Email and Instant Messaging use

- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will only e-mail people I know, or my teacher has approved.
- I will not be involved in sending chain letters.
- The messages I send will be polite, friendly and sensible.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.

Social Networking

- I will not use social networking sites in school.
- I will only accept friend requests with someone I know in the real world and an adult has approved.
- I will not post anything online that I am not happy about being shared with others.

File sharing

- I will not use file sharing software or services.

Mobile phone and hand held gaming devices

- I will not bring a mobile phone to school unless instructed by my parent and agreed by the school.
- I will switch my phone off on entering school grounds.
- I will hand my phone into the office at the start of the school day and collect it at the end of the day.
- I will not bring hand held gaming consoles to school.

Video Conferencing

- I will not initiate, make or answer a video conferencing call
- I will follow agreed rules for video conferencing and our class charter and the school rights respecting actions.
- I will maintain acceptable standards of manners, behaviour and language throughout
- I will avoid causing disruption by – eg. Staying in room throughout whole session and making sure I have visited the toilet before the lesson

- I will listen to whoever is speaking / Take turns to speak / Respect what others say

Tablet use

- I will hold the tablet with two hands.
- I will always sit down when using the tablet (except when making videos).
- I will not lift the tablet off the desk (except when making videos).
- I will turn the tablet's screen off when the teacher is talking.
- I will be gentle when tapping the screen.
- I will use my finger or a stylus on the screen only.
- I will only use the app or website I have been asked to use.
- I will not delete or edit other people's work.
- I will share nicely and stop when my turn is over.
- I will use a laptop or computer when researching and not a tablet.

Consequences

I understand that if I deliberately break these rules, I may not be allowed to use email, the Internet, computers, laptops or tablets and be involved in video conferencing.

There may be additional consequences in line with class rules on inappropriate language or behaviour.

Where applicable, police or local authorities may be involved.

Parents

- Access to the Internet provided to staff and pupils in school has security features but complete security cannot be guaranteed
- The use of the Internet in school is closely monitored by staff
- There will be no use of the Internet without the supervision of staff and that this will be in full view of others, e.g. the classroom, corridor or the library
- Please co-operate with staff, make pupils aware of the rules and expectations within this document
- Parents are reminded that they are responsible for their child's use of online C2k services out-of-school.
- The use of ICT is complimentary to the teaching already done – i.e. the use of computers, laptops and tablets in the classroom is a tool
- Children's full names will not be available online at any stage but some indication of work they do could be added to any online work that becomes available on the school website
- No photographs of pupils will be available online without parents giving their permission
- Parents should discourage pupils from bringing mobile phones to school on the grounds that Internet access becomes very difficult to police
- Parents should also be aware that social networking sites such as Facebook, adhere to a strict 'over 13's' age policy
- Parents are advised to be present if young children are using Gaming sites or social networking sites
- Internet issues will be handled sensitively to inform parents without alarm
- Ensure privacy settings on all devices are set so that only people you or your child knows can view the account.
- Have conversations with your children - talk to them about the benefits and dangers of the internet so that you can empower them to use the internet safely.

- Keep an eye on what your children are doing online and remind them to tell a trusted adult if something happens online that makes them uncomfortable or worried.

- Become a 'net-savvy' parent – safeguard against online dangers by being informed.

- Useful websites and leaflets have been included in the online safety policy (accessed through school website and given as part of school Welcome Pack) providing further advice e.g. getsafeonline.org

School

The school will supervise all internet access. All internet access will be via the C2k filtering system. The teachers will guide pupils towards appropriate materials and where possible check searches and websites. Tasks will be planned and linked to curriculum topics. Children are taught how to use the Internet safely and responsibly through ICT and/or PDMU lessons. Pupils must be informed that internet use is monitored and individual users can be traced and emails are filtered. We encourage the use of email for communication between colleagues in schools and industry, between pupils and teachers, between pupils and pupils. All pupils in year 5, 6 and 7 have an email address created by C2k. Pupils in year 4 (Term 3) and 5 will login with their C2k username and set their own password. In this instance, the teacher will make a note of each child's password. The ICT Leader will also keep a copy of this document, as system administrator. All staff in the school will ensure mobile phones are switched off and not in use during the school day. Teachers using video conferencing must agree to the protocols before a session occurs. A copy of the Three Way Agreement will be displayed in each classroom. In the computer areas there will be displays of the Online safety incident flowchart and CEOP posters. Staff will have clear procedures for reporting online safety issues.

Addendum

Network administrators, ICT Leader and Principal reserve the right to review files and communications to maintain system integrity and ensure that the users are using the system responsibly – they will respect the right to privacy whenever possible.

Any parent or member of staff who wishes to discuss this document can put any questions to:-

Mrs L. Smyth (ICT Leader)

This document is based on:

EU Kids Online September 2011
Using The Mobile Phone in School Handling opportunity and risk appropriately 2010
Anti bullying Network Cyber-bullying sheet for teachers
Cyberbullying DCSF 2007
Acceptable Use of the Internet and Digital Technologies in Schools (DENI circular 2007/1)
Internet Safety (DENI circular 2011/22)
eSAFETY GUIDANCE (DENI circular 2013/25)
Effective Educational Use of Mobile Digital Devices (DENI circular 2016/26)
Online safety (DENI circular 2016/27)

Responsible Internet Use – Permission Form

Please complete, sign and return to the school

Pupil's Name _____

Pupil's Agreement
I have read / my parent or guardian has discussed (in terms I understand) the school's rules for digital technology use. I understand these rules and will use the computer system, digital technologies and Internet in a responsible way and obey these rules at all times.
Signed by pupil:

Class:

Date:

Parent's / Guardian's Consent for Internet Access
I have read, understood and discussed with my child the school rules for responsible use of digital technologies and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. I understand that I am responsible for my child's use of C2k services out-of-school. I will reinforce the following safety precaution with my child.

- Never give out personal information
- Never share your password with others
- Make sure language used is acceptable
- Be polite at all times
- Tell an adult if something on the internet makes you feel uncomfortable or worried
- Choose a user name that does not reflect your real identity
- Avoid chat rooms that are not monitored by moderators

Signed by parent / guardian:

Date:

Parent's / Guardian's Consent for Video Conferencing

I have read, understood and discussed with my child the school rules for responsible use of digital technologies and give permission for my son/daughter to participate in lessons that use Video Conferencing technology.

Signed by parent / guardian:

Date:

Parents and Carers Acceptable Use Policy when using Cumran Primary School's Computer Facilities

General Rules

- **I will respect the hardware and software that is available to me.**
- **I will use the printing facilities in a reasonable way.**
- **I will bring a storage device if I wish to save something.**
- **I will log off and shutdown the computer / laptop when I am finished using it.**
- **I will not install my own software.**

Internet use

- **I am aware that C2k services (school computer system) is monitored and it is my responsibility for appropriate use of my web email account and the Internet.**
- **I will use the Internet in a safe and responsible way.**
- **I will not deliberately seek out offensive materials. Should any appear I will report it to a member of staff immediately.**
- **Attempts to bypass filtering, or to access inappropriate or illegal material will be reported to the school authority.**
- **I will not copy text, images, sounds, animation, videos or music that breaks copyright laws.**

Internet chat rooms and instant messaging

- **I will use social networking sites, chat rooms and instant messaging in a sensible manner.**
- **I am aware that my screen and its content is visible to others.**

Parent and Carers Agreement
I have read and understand these rules and will use the computer system, digital technologies and Internet in a responsible way and obey these rules at all times.

Signed by parent / carer:

Date: