St. Oliver Plunkett PS

eSafety Policy

"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." DENI circular 2007/01

Co-ordinator: Mr Barry Conroy BSc (Hons); PGCE

Introduction

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

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

This policy is largely based on DENI Circular 2007/1 *'Acceptable Use of the Internet and Digital Technologies in Schools'*, DENI Circulars 2013/25 and 2011/22 *'e-Safety Guidance'* and DENI Circular 2016/27 *'Online Safety'* and should also be read in conjunction with the School's Safeguarding policies.

WHAT IS eSAFETY?

eSafety is short for electronic safety.

eSafety highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. eSafety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

eSafety at St. Oliver Plunkett PS:

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

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

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

This eSafety Policy operates in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. eSafety is built into the delivery of the curriculum.

eSAFETY POLICY STATEMENT

Rationale

The staff of St. Oliver Plunkett Primary School recognises the potential of internet use across the curriculum and as such believe:

- The internet provides opportunities to enhance and enrich children's learning experiences across the curriculum
- The internet can present information in new ways, which help pupils to understand, assimilate and use it more readily
- The internet gives pupils access to immediate and up-to-date sources of information
- The internet can motivate and enthuse pupils
- The internet can help pupils focus and concentrate
- The internet has the flexibility to allow pupils to work at their own pace
- The internet offers potential for effective individual/group/whole class work
- The internet gives pupils opportunities to develop skills for life
- The internet provides opportunities to enhance and enrich pupils' learning experiences across the curriculum.

Aims

In order to maximize the potential of internet use in Learning and Teaching and to develop the internet competence of pupils, we aim:

- To raise levels of pupil competence and confidence in using the internet
- To use the internet to enhance and enrich children's learning and add to its enjoyment
- To provide access to electronic sources of information and interactive learning resources
- To enable children and teachers to have access to immediate and up-to-date sources of information
- To develop children's independent learning skills using the internet across the curriculum
- To develop information handling and research skills
- To ensure pupils are aware of the potential dangers of internet use, and how to respond appropriately if they come across inappropriate material
- To ensure internet use is a planned and supervised activity

Roles and Responsibilities

The Role of the ICT Co-ordinator

- To liase with the Principal and staff to revise and update this eSafety Policy as appropriate and where necessary.
- To play a key role in school policy development in relation to internet use and teaching and learning.
- To support and guide colleagues on internet use.
- To contribute to the monitoring and evaluation process.
- To keep up to date with recent developments regarding the internet and advise colleagues appropriately.
- To discuss eSafety with colleagues and as a staff.
- To ensure parental permission for internet use in school is sought.
- To ensure continuing personal and professional development.

The Responsibility of the Classroom Teacher

- To ensure they have an up-to-date awareness of eSafety matters and of the current school eSafety policy and practices.
- To have read, understood and signed the school's Staff Acceptable Use Policy.
- To follow the school's E-Safety Policy and Acceptable Use Policy.
- To report any suspected misuse or problem to the ICT Co-ordinator.
- To ensure digital communications with students (email, Seesaw etc.) are on a professional level only carried out using official school systems. Emails should be sent in accordance with the School's guidance.
- To ensure eSafety issues are embedded in all aspects of the curriculum and other school activities.
- To ensure pupils have a good understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act (1998).
- To monitor ICT activity in lessons, extracurricular and extended school activities.
- To be aware of eSafety issues related to the use of mobile phones, camera and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- To undertake all eSafety training as organised by the school.

Professional Development for Teaching Staff

Training will be offered as follows:

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

The Role of Pupil Digital Leaders

- To help with potential issues regarding eSafety.
- To present information during an assembly on the Safer Internet Day/ Bee Safe.
- To ensure eSafety messages are relayed to classes.
- To help to organise eSafety events and campaigns.

The Responsibility of Pupils

- To ensure they use the school ICT systems in accordance with the Pupil Acceptable Use Policy (Appendix I), which they will be expected to sign before being given access to school's systems.
- To have a good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- To know and understand school policies on the use of iPads (Appendix II).
- To understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the school's eSafety Policy covers their actions out of school, if related to their membership of the school.

E-Safety Education for Pupils

E-Safety education for pupils will be provided in the following ways:

- A planned eSafety programme will be provided as part of their lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Child Exploitation and Online Protection (CEOP) resources will be used as a teaching tool.

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

- Pupils will be helped to understand the need for the student Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

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

- Pupils will be made aware of the importance of filtering systems through the E-Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and to support the eSafety policy outlined by the School.

Parents and carers (Appendix IV) will be encouraged to support the school in promoting good eSafety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events

- online communication with staff

- their children's personal devices in the school

Parents / Carers Training and Support

Parents and carers have an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. The school recognises that some parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School will seek to provide information and awareness to parents and carers through:

- The school website www.stoliverplunkettberagh.com provides links to external sites such as CEOP and Digital Parenting

- Letters, newsletters, websites, Vodafone Digital Parenting leaflets

- eSafety Guidance will be delivered through key events
- Guidance to Parents (Appendix IV).

1. Internet Services

1.1 Connectivity and Filtering

The school has two internet systems in its infrastructure. Internet access is filtered for all users.

1.2 C2K

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

The service allows for Websense filtering giving the school flexible control. Customised filtering is managed by Mr Conroy (ICT Co-ordinator) and he can amend the local filtering policy to the needs and demands of the school. There are a number of agreed locked down sites that can never be overridden by the local school policy.

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

Some of the safety services include:

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

1.3 Classnet

The school installed a BT internet line in January 2017 (Classnet) to enable the large consignment of iPads to access on-line internet services. This Classnet connectivity and filtering system has built in effective firewalls, filtering and software monitoring mechanisms.

The school will take appropriate measures to safeguard non-C2K equipment against security breaches.

1.4 Auditing and Reporting

Filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. The responsibility for the management of the school's filtering policy is held with the Principal and the ICT Coordinator.

They manage the school filtering by:

- Monitoring reports of the use of C2k/Classnet which are available on request.
- Keep records and logs of changes and of breaches of the filtering systems.

Staff and children have a responsibility to report immediately to the ICT Co-ordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

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

- Designated Child Protection Officer
- Board of Governors
- External filtering provider/PSNI on request

2. Internet Safety Awareness and E-Safety Education Programme

We believe that, alongside written eSafety and Acceptable Use policies (AUP), it is essential to educate all users in the safe and effective use of the internet and other forms of digital communication, both inside school and outside school. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

2.1 Internet Safety Awareness for Pupils

A planned eSafety education programme for Years 1-7 takes place through both discrete lessons and wider curriculum opportunities. The school takes part in an e-Safety week in February. Pupils are also encouraged to enter e-Safety competitions, make posters and charts. Information is delivered and reinforced through school posters (Appendix II), the school website, the Digital Leaders, Pupils' Council and the school newsletter (STOP Press). Rules for the Acceptable Use of the Internet (which have been drawn up with the aid of pupils) are discussed with all pupils and are prominently displayed in classrooms. Pupils are made aware of copyright and plagiarism. Pupils are encouraged to validate the accuracy of information which they research. The children are involved in the planning and delivery of E-Safety lessons/assemblies during eSafety week.

Other Resources:

Child Exploitation and Online Protection (CEOP) resources: a useful teaching tool looking at Internet safety and incorporated into our PDMU and ICT programme.

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

Other pupil resources available:
Signposts to Safety, KidSMART, Know IT All for Schools, ThinkUKnow

2.2 Internet Safety Awareness for Staff/ Professional Development

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

E-Safety training is linked with Safeguarding Training. Training needs are informed through audits. The induction programme for new staff includes e-Safety. The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of the Department's policy and strategy on ICT use in teaching and learning and are updated in relation to relevant changes. Staff uphold copyright regulations and intellectual property rights.

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

2.3 Internet Awareness for Governors

Mrs Maguire and Mr Conroy keep governors updated on eSafety and eSafety issues.

2.4 Internet Safety Awareness for Parents/ Carers and the Community

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

available on the school website. Internet safety leaflets for parents and carers (for example, Appendix 4) are sent home annually. Parents/carers' attention is drawn to the school website and school newsletter (STOP Press) where e-Safety messages are given. The school has, on a number of occasions, organised a talk on internet safety, delivered by the PSNI; NSPCC/O2 for parents and the community.

3. Health and Safety

We have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources in the classrooms, and where pupils are supervised at all times. Guidance is issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

3.1 Risk Assessments

Life in the 21st century presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. The school considers all new technologies wisely to ensure that it is fully aware of and can mitigate against the potential risks involved with their use. In so doing, pupils are informed of what to do if they come across inappropriate material or situations online.

3.2 Use of Mobile Phones

Most mobile phones have internet connectivity. Please refer to the school's Mobile Phone and Digital Technologies Policy (Appendix VII) on the use of such. Pupils do not bring mobile phones to school.

3.3 Digital and Video Images

Parental permission is gained when publishing personal images on the website or other publications. All members of the school understand their rights and responsibilities in the taking, use, sharing, publication and distribution of images (and in particular the risks attached). The school gains parental/carer permission for use of photographs or video images (Appendix IV). Staff are allowed to take images to support educational aims. Staff must follow school policies concerning the distribution and publication of such. Pupil names associated with images will not be shared on the school website.

3.4 Cyber Bullying

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

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting occurs in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.
- Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator. Pupils will be reminded that cyber-bullying can constitute a criminal offence.

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

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

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

Policy Review

Internet technology and the school's use of resources will develop and change with time. The school intends to revise and up-date this eSafety Policy when new technologies are introduced and as appropriate and where necessary.

Date

September 2017

Appendix I

St. Oliver Plunkett Primary School

ICT Code of Safe Practice for Pupils

E Safety Rules

✓ I will log onto the school network *My School* Learning Platform with my own user name and password.

✓ I will only use ICT, including the internet, e-mail, iPad, digital video, mobile technologies, etc. for school purposes.

✓ I will only use my class e-mail address or my own school e-mail address when e-mailing.

✓ I will only open e-mail attachments from people I know, or who my teacher has approved.

✓ I will not tell other people my ICT passwords.

✓ I will only open/delete my own files. I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.

✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.

✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

✓ I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my eSafety.

Pupil's Full Name …….... (printed) Class: ……

Pupil's Signature …….……. Date ……

Appendix II

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

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

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

Appendix III: ICT Code of Safe Practice for Staff

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

EMAIL: I will only use the school's email or personal email (if approved by Mr Conroy)/ Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors. (See school's Email Policy). I will use the approved C2k secure e-mail system for school business and communication with parents. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

PASSWORDS: I will comply with the C2K ICT system security and not disclose passwords provided to me by the school or other related authorities.

DATA PROTECTION: I will not give out personal details e.g. mobile phone number/personal e-mail address to pupils. I will ensure personal data is kept secure and used appropriately, whether in school, taken off school premises or accessed remotely. Images of pupils/staff will only be taken, stored and used for professional purposes online with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Principal.

C2K INSTALLATION: I will not install any hardware or software on the C2K system without the permission of Mr Conroy.

USE OF INTERNET AND DEVICES: I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory on the C2K system or iPads. I understand that my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to Mr Conroy or Mrs Maguire (managers). I will respect copyright and intellectual property rights. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

SOCIAL MEDIA: In my private life, I will take great care to ensure posts are appropriate. I will not befriend pupils of the school.

MOBILE PHONES: My phone will be on silent and not used when my duty is to be with the pupils.

I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

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

Staff Member:…… Signature …….…….

Job Title: ……..... Date ……..……..…

Appendix IV: Parental Consent Form

Parental Agreement/Consent Letter

Dear Parent

It is essential that pupils are aware of eSafety and know how to stay safe when using Information and Communications Technology (ICT). As part of St. Oliver Plunkett PS's ICT programme, we offer pupils supervised access to a *filtered* Internet services provided by C2k (PCs & laptops) and by Classnet (iPads). Access to the Internet will enable pupils to explore and make appropriate use of many websites that are of enormous educational benefit. They can also exchange messages with other Internet users throughout the world. However, in spite of the tremendous learning potential, you should be advised that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service providers have installed filtering software which operates by blocking thousands of inappropriate websites and by barring inappropriate items, terms and searches in both the Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

The school's rules for safe Internet use accompany this letter. Please read and discuss these with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please make contact.

Yours sincerely,

Barry Conroy
UICT Co-ordinator

---

e-Safety Acceptable Use Rules Return Slip 2017-2018

Pupil / Parent Agreement:

We have read and discussed the rules and confirm that we have understood what they mean.

Pupil's Signature _____ Class _____

Parent's Signature _____ Date _____

Appendix V: Internet Access - Additional Advice for Parents

1. A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.

2. Parents should agree with their children suitable days/times for accessing the Internet.

3. Parents should discuss with their children the rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use.

4. Parents should get to know the sites their children visit and talk to them about what they are learning.

5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below).

6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities.

7. 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.

8. 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.

Further advice for parents is available from the following sources:

- http://www.thinkuknow.co.uk Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.
- http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.
- http://www.parentscentre.gov.uk/usingcomputersandtheinternet A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.
- http://www.bbc.co.uk/webwise Includes an 'Internet for Beginners' course and a tool for answering your internet related questions.
- http://www.kidsmart.org.uk/ Explains the SMART rules for safe internet use and lots more besides.
- http://www.ceop.gov.uk/ The government's Child Exploitation and Online Protection Centre (CEOP)
- http://www.parents.vodafone.com Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use

Appendix VI: Use of Mobile Phones and other Electronic Devices

Rationale

The Board of Governors of St. Oliver Plunkett PS wishes to ensure that all pupils are safe and well cared for. All staff and pupils have a right to work, enjoy and learn in a secure and caring environment. They also have a responsibility to contribute to the protection and maintenance of such an environment. The use of increasingly sophisticated equipment and integrated cameras could present a number of problems, hence, the co-operation of parents and carers with this guidance is very much appreciated.

It is therefore school policy to prohibit the unauthorised use by pupils of mobile phones or other electronic devices while on our school premises, grounds or on trips or activities e.g. school swimming.

Guidance

The school will adhere to the following guidance:

- While we fully acknowledge a pupil's right to have a mobile phone or other electronic device, we discourage pupils from bringing them to school. They are valuable items and might be vulnerable to damage, loss or theft. There is also the potential for inappropriate behaviour and potential bullying which could be harmful to other pupils or staff. Many have built - in cameras which could lead to child protection and data protection issues with regard to inappropriate photographs or distribution of images. We have a duty to protect all members of our school community.

- In an emergency situation, and with the express approval of a senior member of the school staff, or where a written request has been received from the parent/carer, the device may be stored in the school office. It is the child's responsibility to ask for the device at the end of the school day. Should parents need to contact pupils, or vice versa, this should be done following the usual school procedures: via the school office (028 80758594).

- Pupils may only take photographs on school devices as part of a supervised educational activity which has been authorised by a senior member of staff.

- The school accepts no liability for the loss or damage of any electronic device which is in the pupil's possession during the school day.

- If a pupil is found by a member of staff to be using a mobile phone/electronic equipment for any purpose, the device will be confiscated from the pupil. The pupil must arrange for their parents/guardians to collect confiscated equipment from the School Office during normal working hours.

- Inappropriate photographs or video footage with a mobile phone or other electronic device of other pupils or teachers will be regarded as a serious offence and disciplinary action will be taken.

This policy supports the school's Health and Safety and Safe Guarding Policies: Anti-bullying, Child Protection, Positive Behaviour and Internet Acceptable Use policies. It has been endorsed by the Board of Governors and will be monitored, reviewed and amended as required.

Appendix VII: Email Policy

This policy operates in conjunction with the E-Safety Policy.

Rationale

Email is a useful communication tool which can be used to support daily workload. Staff using email do so at their own risk. To minimise risks, staff use of the internet and emails is governed by this policy.

Areas where legal problems or a crime may arise:

Pornography	Harassment	Copyright	Contracts
Defamation	Confidentiality	Use of images	Personal use

This policy is to protect staff and pupils in school. The ICT Co-ordinator, Mr Conroy, has a responsibility to support and educate staff in the safe use of the internet for email purposes and to ensure that staff do not unwittingly get involved in some activity that would bring the school into disrepute.

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

Good Practice

- Email accounts should be checked daily
- The School email system is primarily for educational purposes. Communication with colleagues should be through the c2k account.
- All emails with parents should be through the school's email system and should be professional in nature
- Emails should be brief, with a clear subject field entry. Take care with spelling and punctuation.
- Do not criticise by email; this can be very offensive on screen.
- Always assume your email will be forwarded on to someone.
- An email should not include sensitive personal data e.g. alleged offences, beliefs
- Be careful when opening attachments; they may be infected with a virus
- Log out/lock when leaving iPad/PC to prevent unauthorised use of your email account.
- Email alerts should be turned off in school, especially if you are displaying your screen on the board.
- Do not forward material via email that is in breach of copyright. Failure to comply with this policy may lead to disciplinary action.

This policy may be amended at any time. Staff will be informed of any amendments.

Appendix VIII: Password Policy

Rationale

Password security is one of the most important skills in online safety. A strong password is a first line of defence against intruders and imposters. We believe it is important to begin teaching password security principles as soon as pupils begin using ICT. Users may only access the C2K network and devices through a properly enforced password protection policy.

The C2k account will be "locked out" following successive incorrect log-on attempts

C2k Staff Passwords

- Staff are expected to have secure passwords which are not shared and changed periodically.
- All staff have unique names and passwords
- Password must be at least 8 characters long (any characters and/or numbers)
- Password must not have been used before
- Password cannot be reset within 2 days by the User.
- Individual pupil passwords can be reset by C2k Manager
- Passwords will expire in 120 days

Pupil Passwords

- All pupils have a C2K Password. In Years 1 and 2 Pupils are issued a simplified C2K password such as: User name: Peter; Password: Peter.
- In Years 3-6 pupils log on with their names e.g. User name: rblack123 and Password* where * is a number.
- In Year 7 pupils log on with their names e.g. User name: rblack123 and they have a password of their choice.
- The system prompts them to change their password regularly.
- Pupils are taught not to share their password with anyone.
- All pupils can have their work tracked using their unique user names and passwords

Appendix IX: Classnet Filtering

This policy has been adopted from iTeach by St. Oliver Plunkett PS Beragh.

Classnet Internet WiFi Filtering

The school's classnet wifi and infrastructure has been installed and is maintained with an active, monitored filtering system to satisfy both the needs of child protection and inappropriate content whilst ensuring that it serves to support teaching and learning.

The school through detailed testing identified that it required a dedicated internet service to support its mobile device strategy. This system exists in parallel to all C2K infrastructure. In line with DENI Circular provision, the school has ensured that this additional service is:

a) Filtered to standardised child protection levels
b) Supported by trained staff in its use
c) Reported to and approved by its Board of Governors.

Scope of document

This document details all aspects of the filtering policy and systems for 'the network', also referred to here as 'Classnet'.

Access to network

Access to the network is provided through password authentication using WPA. This key is available to Mr Conroy and access is governed by unique device registration. No devices can join the network without this approval and authentication. Access is provided subject to the terms of the school's Internet Acceptable Use Policy and its e-Safety Policy.

Hardware and General Service Provision

The following has been installed and configured in school to ensure only appropriate content is available to all users:

1. A hardware firewall filter is installed which intercepts all Internet traffic leaving and entering the school network and this cannot be circumvented. This firewall appliance is configured for the Globalview Internet filtering service, powered by industry giant Cyren. This service is a professional, commercial category based web filtering solution in use by over 120,000 schools worldwide. It uses a category based system to group web sites in addition to keyword, IP and specific white and blacklist control. School licenses are purchased on a fixed three year term to ensure continuity of service and the individual firewall is monitored 24/7 with instant notification of any concerns.
2. A server is installed which filters by Domain Name Service (DNS) provision, which provides granular control for content and ensures compliance with 'Safe Search' browsing which ensures that only images deemed appropriate for pupils can be displayed on any web search. This allows the school to rapidly make any filtering changes should a third party (e.g. Google) make any changes to its service.
3. In addition, IP and URL black and white listing is supported locally which ensures any content that is flagged as non-desirable on the network, can be disabled immediately
4. Full access logs are maintained for all traffic and all attempts at access of inappropriate content
5. A remote monitoring system to ensure that filter licensing is at all times monitored and active.

Specifics of Filtering Service

This filtration service uses a category based system to decide if a website is viewable from all Internet connected devices.

The Primary Categories include:

- Child Protection (including violence, porn, weapons etc)
- Leisure (entertainment, travel, sports)
- Business
- Chatting (internet chatting and instant messaging services)
- Computer & Internet Services (social networking, streaming, spam sites)
- Other (image sharing, dating and person, compromised, including uncategorised)

If a website falls into a category that is not deemed acceptable for use in the classroom, the user will be subject to viewing an 'unsuitable' notification on the web browser and this activity logged to user and device level.

Cyren independently search the Internet using their tools to select what category is assigned to any available website. This is then matched to the live filtering within the school.

A website's category can be manually checked and identified by using their free, up to date database tool: http://www.cyren.com/url-category-check.html

Additional Filtering

To supplement category based filtering, the school maintains a rolling list of websites requested by teaching staff, checked and approved to be exempt from category filtering and this is available in school. This list is maintained by the ICT coordinator. Websites are added to a specific blocking list where required.

Safe Search

The school has deployed Google 'Safe Search' by default on all devices on the network. This cannot be bypassed and ensures images are at all times appropriate for school use. This system is constantly monitored and active.

Logging

All traffic in and out of school is monitored and logged. Logs are available on request to the Principal and designated child protection officer. Each log can be narrowed to a device and user and is date/time stamped with details of any accessed URL. The school also has 'flagging' enabled which automatically informs the designated staff member of any attempts to access an inappropriate (i.e. filtered) site.

School Procedures

The school has a mechanism should a website be found to be uncategorised, and can request a category to be allocated from within the URL category tool. Individual websites and iOS apps can be permitted through the filtering system on a site per site basis using a system called White Listing. This is particularly useful when blocking such apps as Twitter, Facebook and Tumblr that operate within an 'App' environment.

Additional Filtering for Mobile Devices

Standard browsers are removed (e.g. Safari) and is replaced by a secure browser which adds a second filtering level per device. This is controlled on age based settings and is secondary to the firewall filtering. No pupil can access an unfiltered browser. All devices are supervised which enables Internet access control at OS level, which offers a final layer of filtering based in content groups and discrete Internet addresses.

Checking and Maintenance

The entire wifi provision is checked constantly via remote systems, and is manually checked monthly on site to ensure it consistently adheres to the processes in this document.

Further notes

• Filtering has been checked by two staff within DENI Guidelines.

• Two members of staff have been trained in filter use in order to react with speed for any system issue

• The network is supported on demand/under contract from an external agency (iTeach)

• The school e-Safety Policy and Internet AUP has been changed to match these changes and systems.

Procedure for Schools on notice of an Incident relating to Filtering on Classnet

Introduction

iTeach uses commercially provided services to filter and restrict access to any internet content, which is incompatible with the ethos and public standing and protection of children and vulnerable adults. To this end, Classnet is installed to protect against the use of school resources in accessing inappropriate internet content. However, on rare occasions, there may be cases whereby a user may gain access to material that is deemed inappropriate in a school setting.

This procedure has been developed to ensure that all schools who use iTeach's Classnet system are aware of the procedure to follow if they have received any complaints directly related to the use of the internet, or if they receive a complaint in relation to a web site, search, image or video that has been accessed.

Access to Services

The iTeach network is monitored constantly and access is logged and all reported issues can be investigated as the need arises.

Reporting Responsibilities

Responsibilities for the school

- Protection of all children is everyone's responsibility and it is important that potential breaches are reported to iTeach so that the incident can be resolved within a reasonable period.
- If a school or member of iTeach staff receive any complaints in relation to internet content, then they should report this incident to the iTeach Designated child protection officer (DCPO) who will then work on resolving the issue.
- The device in question should be retained by the school DCPO in case further inspection is needed
- The details of the complaint should be sent in the first instance via email to dcpo@iteach-uk.com and must include all of the following information:

    • School name
    • Email address of the school DCPO
    • Date and time of incident
    • Device
    • Confirmation of Classnet system in use
    • Nature and description of image or web site
    • If a web site - the URL shown in the browser
    • If an image the search term used

iTeach process

- Confirmation of receipt of complaint
- DCPO passes to the iTeach Technical Manager
- Immediate check of standard filter in place, and confirmed to the school thus ensuring that all devices are secure
- Confirmation if action can be taken to block the material of concern
- Blocking of material where possible
- Written confirmation to school
- Closure of incident

Responsibilities for iTeach staff

- iTeach commits to providing an issue resolution within **48 hours**
- On receipt of notification the DCPO will pass details directly to the iTeach Technical Manager
- The DCPO will confirm receipt with the school **by return email**
- The DCPO will retain a written record both electronically and in hard copy
- The iTeach Technical Manager will work to investigate the incident and will contact the Principal of the school **within 4 hours** and inform them of the steps required to rectify the situation and approximately how long it will take.
- The iTeach Technical Manager will:
    - Check the current filter integrity and document
    - Confirm that the image or site in question can/cannot be accessed on Classnet
    - Put in place filtering, where possible to prevent this from occurring
- The Technical Support team will deal with this complaint as a priority and the school notified of status on a regular basis **(at minimum once daily)**. The school may request a progress report by contacting the Technical Team at any stage.
- Logs, where requested, must be supplied to school
- When the issue is resolved the Technical Manager, will notify the Principal that the status is complete and provide the school with a report, detailing that nature of the complaint, why this occurred and what iTeach have done to rectify the situation, both the long term and short term measures, and check with the school that they are happy with the outcome.
- All communication must be in writing, via email and be copied to dcpo@iteach-uk.com
- Any escalation required should be documented to The Managing Partner, iTeach.
- The attached document checklist should be completed by the relevant staff and returned to the DCPO

NOTE: If the content of the complaint appears to offer illegal services such as child pornography, iTeach will report this to the Internet Watch Foundation [http://www.iwf.org.uk/] website. This organisation works in partnership with ISPs, Telcos, Mobile Operators, Software Providers, Police and Government, to minimise the availability of illegal Internet content, particularly child abuse images.

Identification of Hazards (i.e. What could reasonably be expected to cause harm)	Identification of Risks (i.e. Who might be harmed in what ways)	Existing Control Measures (i.e. What devices or procedures are in place to reduce or control the risk)	Risk Evaluation (i.e. How dangerous, how likely) (PTO for example of risk evaluation calculation)				Further Action Planned or Required To Control OR Reduce Risk
			Likelihood of Harm (1-5)	Probable Severity (1-5)	Calculated Risk (1-25)	Low (1-8) Medium (9-14) High (15-25)	
Access to inappropriate content through the Internet	Staff and pupils may attempt to access inappropriate content through the Classnet network	The following has been installed and configured in school to ensure only appropriate content is available to all users: The Classnet network conforms to all DE guidelines for filtering. A hardware firewall filter is installed which intercepts all Internet traffic leaving and entering the school network and this cannot be circumvented. Additional Information: This firewall appliance is configured for the Globalview Internet filtering service, powered by industry giant Cyren (previously Commtouch). This service is a professional, commercial category based web filtering solution in use by over 120k schools worldwide.	2	2	4	Low	Access to the network is provided through password authentication using WPA. This key is not available to any staff. Access is therefore governed by unique device registration and pre-approval by iTeach staff only. No other devices can join the network without this approval and authentication.

Identification of Hazards (i.e. What could reasonably be expected to cause harm)	Identification of Risks (i.e. Who might be harmed in what ways)	Existing Control Measures (i.e. What devices or procedures are in place to reduce or control the risk)	Risk Evaluation (i.e. How dangerous, how likely) (PTO for example of risk evaluation calculation)				Further Action Planned or Required To Control OR Reduce Risk
			Likelihood of Harm (1-5)	Probable Severity (1-5)	Calculated Risk (1-25)	Low (1-8) Medium (9-14) High (15-25)	
Continued… Access to inappropriate content through the Internet	Continued… Staff and pupil users may attempt to access inappropriate content through the Classnet network	Continued… All of the iPads have restricted access to the Internet by the filtering been set on their use of the internet browser Safari. In their use of the Classnet network, staff will abide by the school's iPad Acceptable Use Policy and the E-Safety Policy. In their use of the Classnet network pupils will abide by the school's iPad Code of Conduct.	2	2	4	low	Pupils may only use the iPads under staff supervision. Acceptable use of iPad procedures have been signed by all staff and pupil users. (see attached procedures for pupils and staff)

Identification of Hazards (i.e. What could reasonably be expected to cause harm)	Identification of Risks (i.e. Who might be harmed in what ways)	Existing Control Measures (i.e. What devices or procedures are in place to reduce or control the risk)	Risk Evaluation (i.e. How dangerous, how likely) (PTO for example of risk evaluation calculation)				Further Action Planned or Required To Control OR Reduce Risk
			Likelihood of Harm (1-5)	Probable Severity (1-5)	Calculated Risk (1-25)	Low (1-8) Medium (9-14) High (15-25)	
Use of inappropriate apps	Staff and pupil users may attempt to download and use inappropriate Apps from the Apple store on the iPad devices	In their use of the iPad devices and Apps, staff will abide by the school's Acceptable Use Policy and E-Safety Policy. In their use of the iPad devices and Apps, pupils will abide by the school's Code of Conduct. Access to the school's Apple store account is restricted to the Principal and class teachers. Only the Principal and the ICT Coordinator may purchase and download Apps to the school's iPad devices. The Principal will use the mobile device management service, Meraki, to track and manage the iPad devices. This monitors what Apps are on each device, when they are used, their location and the storage used. See Link (https://meraki.cisco.com/) The school's ICT coordinator has been trained in the use of Meraki.	2	2	4	low	Pupils may only use the iPads under staff supervision. Acceptable use of iPad procedures have been agreed and signed by all staff and pupil users. (see attached documents) The Meraki mobile device management service will be monitored on a weekly basis by ICT Coordinator and the Principal

Multiply the **LIKELIHOOD OF HARM (1–5)** by the **PROBABLE SEVERITY (1-5)** to **CALCULATE THE RISK (1-25)** and then clarify as **LOW (1-8)**, **MEDIUM (9-17)** or **HIGH (18-25)**

LIKELIHOOD OF HARM	**X**	**PROBABLE SEVERITY**	**=**	**CALCULATED RISK RATINGS**
1 very unlikely		1 trivial injury		LOW (1-8)
2 unlikely		2 minor injury		MEDIUM (9-17)
3 50/50 likelihood		3 moderate injury		HIGH (18-25)
4 likely		4 major injury		
5 very likely		5 fatality		