MULLAVILLY PRIMARY SCHOOL

'Inspiring, Believing Achieving'

E-Safety Policy

and Acceptable Use Agreement

October ***2017***

Review Date

October 2019

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

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

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

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

This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Mullavilly Primary School.

Care and responsibility

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. With these opportunities we also have to recognise the risks associated with the internet and related technologies.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorized access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

As with all other risks, it is impossible to eliminate the risk completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with any scenarios which may arise.

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

This document should be used in conjunction with a range of other school policies and guidelines including the Keeping Safe Policy.

The Internet

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

Potential Contact

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

Children should be taught:

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

Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content.

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

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

Children should be taught:

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

Excessive Commercialism

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

Children should be taught:

- Not to fill out forms with a lot of personal details.

- Not to use an adult's credit card number to order online products.

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

Roles and Responsibilities

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

The Principal/CT Co-ordinator have the responsibility to update Senior Management and Governors with regard to e-safety and all governors should have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the e-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff and pupils, is to protect the interests and safety of the whole school community.

It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed bi-annually.

E-Safety Coordinator

The E-Safety Coordinator, Mrs E Riddle, will takes day to day responsibility for E-Safety issues and have a leading role in establishing and reviewing the Schools policies/documents.

The E-Safety Coordinator will:

- Ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provide training and advice for staff
- Liaise with C2K and iTeach
- Liaise with the EA and DENI on E-Safety developments
- Liaise with the technical staff
- Receive reports of E-Safety incidents and create a log of incidents to inform future E-Safety developments
- Meet with Head of Pastoral Care to investigate abuse of social network sites by pupils
- Attend relevant meetings with Board of Governors

- Discuss current issues, review incident logs
- Monitor and report to senior staff any risks to staff of which the E-Safety coordinator is aware

The Child Protection Officer

The Child Protection Officer and deputies will be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data (Appendix 9)
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Network Managers

The Network Managers will monitor that C2K e-safety measures, as recommended by DENI, working efficiently within the school to ensure that:

- The C2k/ITeach operates with robust filtering and security software
- Monitoring reports of the use of C2k / ITeach are available on request
- The school infrastructure and individual workstations are protected by up to date virus software.
- The school meets required e-safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with E-Safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- Software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- The “administrator” passwords for the school ICT system, used by the Network Managers are available to the Principal and kept in a secure place

Teaching and Support Staff

E-Safety Skills’ Development for Staff:

- All staff receive regular information and training on e-Safety issues through the co-ordinator at staff meetings.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

- New staff members receive information on the school's Acceptable Use Agreement as part of their induction.

- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

Pupils

Are responsible for ensuring that:

• They use the school ICT systems in accordance with the Pupil Acceptable Use Policy (Appendix 1), which they will be expected to sign before being given access to school's systems.

• They have a good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.

• They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• They know and understand school policies on the use of iPads (Appendix 2), mobile phone, digital cameras and hand held devices (Appendix 7). They should also know and understand school policies on the taking / use of images and on cyber-bullying.

• Pupils are introduced to email and taught about the safety of using e-mail both in school and at home (Appendix 10)

• They understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety 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:

• E-Safety 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. Keeping Safe resources and the website www.thinkuknow.com 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; they will also be warned of the consequences of attempting to subvert the filtering system.

Parents/Carers

E-Safety Information for Parents/Carers:

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used on the school website.
- The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.
- The school will communicate relevant e-Safety information through newsletters and the school website.
- This policy is available to parents via the school website, a hard copy can be obtained form the school office.

Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use.

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Teaching and Learning

Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff.
- The school Internet access is filtered through the C2k managed service and iTeach.
- No filtering service is 100% effective; therefore, all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

E-mail: (Appendix 10)

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children are not always given individual e-mail addresses. In some instances, children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

Social Networking: (Appendix 12)

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

Mobile Technologies: (Appendix 7)

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to use personal mobile devices/phones (in school) during class.
- Staff should not use personal mobile phones during designated teaching sessions.

Managing Video-conferencing:

- Videoconferencing will be via the Capita network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Networks: (Appendix 13)

- Pupil access to the Internet is through a filtered service provided by Capita and iTeach, which should ensure educational use made of the resources is safe and secure, protecting users and systems from abuse. Parental permission is sought from parents before pupils access the Internet.

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 as well as the e-Safety 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.

The following legislation covers different elements of cyber-bullying behaviour:

Protection from Harassment (NI) Order 1997 http://www.legislation.gov.uk/nisi/1997/1180

Malicious Communications (NI) Order 1988 http://www.legislation.gov.uk/nisi/1988/1849

The Communications Act 2003 http://www.legislation.gov.uk/ukpga/2003/21

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

Publishing Pupils' Images and Work

The school website is www.mullavillyps.co.uk. We intend to use galleries and articles showcasing both pupils' work the pupils themselves. When posting photographs to the site, we will ensure that:

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

- Parents/carers may withdraw permission, in writing, at any time.

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

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

- Groups or group activity photographs used on website.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Policy Decisions

Authorising Internet access:

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms.
- Access to the Internet will be supervised by the class teacher.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security: (Appendix 11)

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.

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
- Individual pupil passwords can be reset by C2k Manager
- Passwords will expire in 90 days

Pupil Passwords

- All pupils have a C2K Password. In Years 1-3 Pupils are issued a simplified C2K password such as User name: Zoe Password: Zoe.

- In Years 4-6 pupils log on with their names e.g. User name: rblack123 and a password set by the teacher.
- In Year 7 pupils 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.
- Some pupils also have passwords for Software programmes.

Handling e-Safety Complaints (Appendix 14)

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/iTeach which are available on request.
- Keep records and logs of changes and of breaches of the filtering systems.
- These changes and breaches should be reported to the E-Safety Coordinator.

Staff and children have a responsibility to report immediately to the E-Safety Coordinator 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:

- E-Safety Coordinator
- Principal and Board of Governors
- External filtering provider/PSN on request

Actions and Sanctions

Pupil Incidents

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

Reporting Pupil Incidents

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

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

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

STEPS TO FOLLOW WITH PUPIL INCIDENTS

1. In the first instance, issues should be reported to and documented by The E-Safety Co-ordinator.

2. The issue should be relayed to the Principal and, where necessary, the Child Protection Officer and Deputy Officers.

Sanctions for Pupils Incidents

Minor school related incidents (whether in school or out of school) will be dealt with by the Principal and the Senior Leadership Team. This may result in parents being informed, a temporary ban on Internet or device use and/or a loss of Golden Time/ Club Time. Incidents of technology misuse which arise will be dealt with in accordance with the school's Behaviour Policy. Parents will be informed of breaches of contract and /or failure to handle devices carefully.

Incidents involving Child Protection Issues

Incidents involving child protection issues will be dealt with in accordance with the school's Safe Guarding Child Protection Policy. Parents and where necessary, PSNI, Social Services, Governors will be informed.

Staff Incidents and Reporting

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

The Code of Conduct is brought to all staff on an annual basis. All staff are asked to read through the code of conduct and sign on an annual basis.

Any breach of the staff code of conduct, e-safety or social media policy will be dealt with by the principal and/or governors.

Staff Sanctions

Governors will deal with breaches of policy by the staff.

Governors will refer to the DE Governor's Handbook.

Governors will take advice from appropriate authorities.

Governors will follow the EA Disciplinary Guidelines.

Code of Safe Practice

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

The school has:

(a) a Pupil Code of Practice (Appendix 1); and

(b) a Staff Code of Safe Practice (Appendix 3)

containing e-Safety Rules which makes explicit to all users what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, iPads (Appendix 2) and digital video equipment. It should be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones) are subject to the same requirements as technology provided by the school.

The ICT Co-ordinator and the Senior Management Team will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Safe Practice for Pupils

A parental/carer consent letter (Appendix 4), accompanied by the Code of Practice for pupils is issued to parents/carers at the beginning of the new school year. This consent must be obtained before the pupil accesses the internet.

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

The school's e Safety Code of Practice for Use of the Internet and other digital technologies is made explicit to all pupils;

- E-Safety guidelines are displayed prominently throughout the school (Appendix 6);

- Pupils and their parents/carers are asked to sign the Code of Conduct sheets;
- Pupils, using the Internet, will normally be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and supervised;
- Pupils will, wherever possible, use sites pre-selected by the teacher and appropriate to age group;
- Pupils are educated in the safe and effective use of the Internet, through a number of selected websites, including www.thinkuknow.com.

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

Use of mobile phones by pupils is not permitted on the school premises during school hours. (Appendix 7)

Code of Safe Practice for Staff

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

- The Code of Safe Practice has been agreed with staff (Appendix 3).
- Pupils accessing the Internet should on the whole be supervised by an adult at all times.
- Staff will make pupils aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately the Principal.
- Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of pupils should, where possible, be taken with school equipment and images stored on the external school storage device, accessible only to staff or under supervision for pupil work.
- School systems may not be used for unauthorised commercial transactions.
- Staff are expected to have secure passwords which are not shared and changed periodically.
- A Staff Safe Code of Conduct, which details sanctions, is signed by all staff.

Communicating the Policy

Introducing the e-Safety Policy to pupils:

- e-Safety rules (Smart Tips) will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/Keeping Safe lessons.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety Policy:

- All staff will be given the School e-Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop or iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the Governors' responsibility and they will review its effectiveness bi-annually. They will do this during reviews conducted between the ICT Co-ordinator and Designated Child Protection Co-ordinator.

This policy should be read alongside the following school policies: Pastoral Care Policy, Positive Behaviour Policy, Child Protection Policy, Anti Bullying Policy, Health and Safety Policy and the ICT Policy.

Appendix 1: ICT Code of Safe Practice for Pupils

E Safety Rules

- I will log onto the 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 through an online activity 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 e-Safety.

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

Pupil's Signature ……..……. Date ……

Appendix 2: Acceptable Use of iPads

Appendix 3: 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 the E-Safety Coordinator or Principal.

- EMAIL: I will only use the school's email or personal email/ Internet / 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. Personal data will only be taken out of school or accessed remotely when authorised by the Principal. Such data must be encrypted. Images of pupils/staff will only be taken, stored and used for professional purposes online 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 the Principal.
- 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 the Principal or ICT Coordinator. 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 (see Social Media Policy). I will not befriend pupils of the school.
- MOBILE PHONES: My phone will be on silent and not in use 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.

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

Appendix 4 (1): Parental Consent Forms

Dear Parent/ Carer

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

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

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

Please read through the accompanying leaflets with your child and ensure your child understands these. If you have any concerns or would like some explanation, please contact Mrs McClimonds.

Pupil: _____ Class: _____

We have discussed the information in the Code of Safe Practice for Pupils.

…….... (child's name) agrees to follow the e-Safety rules and to support the safe use of ICT at Mullavilly Primary School.

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

Appendix 4(2)

Parent's Name: _____

Pupils' Name: _____

Parent/Carer Acceptable Use Agreement

Digital technologies including the iPad and the computer are integral in the lives of our children, both within and outside school. These technologies provide powerful tools, which open up learning opportunities, stimulate discussion and promote creativity. The pupils have an entitlement to safe internet access at all times.

This acceptable use agreement is intended to ensure:

- That pupils will be responsible users and stay safe while using the internet
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of their children with regard to online behaviour.

The school will try to ensure that your child has good access to digital technologies to enhance learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil's Code of Practice is attached so that you are aware of the school's expectations.

Parents are requested to sign the permission form to show their support.

- I understand that my son/daughter has signed the Code of Safe Practice Agreement
- I understand my child receives online safety education to help him/her stay safe online.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure my child will be safe online. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed online.
- I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have any concerns about any possible breaches of the agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have any concerns over my child's online safety.

Signed: _____

Date: _____

Appendix 4(3)

Pupil: _____

Class: _____

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Pupils and staff may take images for use in lessons or as evidence of learning. Images may also be used to celebrate success in publications, newsletter, on the school website and occasionally in the public media.

The school complies with the Data Protection Act and requests permission before taking images We do not publish pupils' names on the school website beside images or in the newspaper. If a pupil wins an award, we will seek your permission before naming your child in the newspaper.

In accordance with guidance from the Information Commissioner's Office (ICO), parents/carers are welcome to take digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act).

To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the images.

Parents/Carers are requested to sign the permission form below on their child's first year at school to allow the school to take and use images of their children and for the parents/carers to agree.

As the parent/carer of the above named pupil, I agree to the school taking and using digital/video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

YES/NO

I agree that if I take digital or video images at or of school events which include images of other children, other than my own, I will abide by these guidelines in my use of images.

YES/NO

Signed: _____ Date: _____

Appendix 5: 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 6: Samples of Classroom E-Safety Posters

Appendix 7: Use of Mobile Phones and other Electronic Devices

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

Rationale

The Board of Governors of the Mullavilly Primary School wish 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.

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 10: 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 and personal use.

This policy is to protect staff and pupils in school. The e-safety Co-ordinator 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, VLE 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.
- Personal e-mail accounts must not be installed through the Mail app on the iPad but can be accessed through Safari.
- 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
- Ensure information being sent is secure. At present, attachments can be password protected but not the content of an email
- 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. October 2017

Appendix 11: Password Policy

This policy operates in conjunction with the E-Safety 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.
- Individual pupil passwords can be reset by C2k Manager.
- Passwords will expire in 90 days.

Pupil Passwords

- All pupils have a C2K Password. In Years 1-3 Pupils are issued a simplified C2K password such as User name: Zoe Password: Zoe.
- In Years 3-6 pupils log on with their names e.g. User name: rblack123 and a password set by the class teacher.
- In Year 7 pupils 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.
- Some pupils also have passwords for Software programmes.

Appendix 12: Social Media Policy

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

Rationale

This policy is to safeguard and minimise the reputation of the school, staff and the wider community through the use of social media. It applies to the use of social media for work and personal purposes, on equipment used by staff inside school or at home (including non-school appliances). The policy wishes to make sure staff are not making themselves vulnerable.

Scope of Policy

This policy covers all staff, pupils, governors, volunteers, placement students. They will be collectively referred to as Staff in this policy. Parents or community users who have access to our equipment are also required to comply with this policy.

This policy deals with the use of all forms of social media, including Facebook, You Tube and Twitter, and all other social networking sites, internet postings and blogs. It applies to use of social media for school purposes as well as personal use that may affect the school in any way.

1. Personal/ Private Use of Social Media

Staff are permitted to use social media for personal purposes, outside of school working hours.

2. Guidelines for Responsible Use

Staff must not post disparaging or defamatory statements about:

1. The school

2. Current, past or prospective Staff (as defined in this policy)

3. Current, past or prospective pupils or their parents/carers/families

4. The school's suppliers and service providers; and

5. Other affiliates or stakeholders

Staff should avoid social media communications that might be misconstrued in a way that could damage the school's reputation, even indirectly. Staff should be respectful when making any statements.

Ensure profile and any content posted are consistent with the professional image you present.

If you disclose your affiliation with the school on your profile or in any social media postings, you must state that your views do not represent those of your employer.

Staff should not accept as a 'friend' any pupil currently enrolled at the school or any past pupil under the age of 18. The exception to this is if the pupil is a family member. Staff should exercise their own discretion in this case.

Staff should ensure that their settings on social media are set in such a way that protects their privacy. This applies to all postings, photographs and images.

Social Media: Prohibited Use

a. Avoid communications that could damage the school's reputation, even indirectly.

b. Do not use social media to defame or disparage the school, management, staff, or any third party

c. Do not use social media to harass, bully or unlawfully discriminate against staff or third parties

d. Do not use social media to make false or misleading statements

e. Do not use social media to impersonate colleagues or third parties

f. Do not express opinions on the school's behalf, unless expressly authorised to do so

g. Do not include the school logo in any posting or in your profile

h. Do not post comments about pupil performance

Any misuse of social media should be reported to E-Safety Co-ordinator.

Breach of Policy

The school does not discourage staff from using social networking sites. However, breach of this policy may result in disciplinary action.

You may be required to remove any content that the school considers to constitute a breach of this policy.

Failure to comply may result in disciplinary action.

Appendix 13: Classnet (ITeach) Filtering

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

This policy has been adopted from iTeach by Mullavilly Primary School Classnet Internet Wi-Fi Filtering

The school's classnet Wi-Fi 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. No devices can join the network without this approval and authentication. Access is provided subject to the terms of the school 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 Global view 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 '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

The default categories selected are as follows:

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 e-Safety coordinator. Websites are added to a specific blocking list where required.

Safe Search

The school has deployed Google 'Safe Search' and Bing Non Explicit image 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 Wi-Fi 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.

Filtering for Email

The school has deployed Google Apps for Education email:

1. Pupil accounts are accessible by designated school officers on request

2. All outgoing email has automated compliance footers

3. Incoming and outgoing mail is filtered for offensive words, terms, content, links and images

4. Provides notification for any attempted breach of item 3 to the designated school officer

Further notes

• Filtering has been checked by two senior 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 ITeach

<u>Introduction</u>

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 ITeach 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 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. In addition, this document applies to the circulating, receiving or sending of inappropriate material via email.

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

A proforma is attached to this document which will provide guidance on all details required and where to send the completed document.

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 occuring

• 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.

Appendix 14

Filtering Incident Form

Name of submitter: _____

Date summited: _____

Date of incident: _____

Time of incident: _____

Device (eg IPad, Laptop): _____

Conformation of C2K of ITeach filtering system in use: YES/NO

Nature and description of image or website:

_____
_____
_____
_____

If a website, the URL shown in the browser:

_____

If an image, the search term used:

_____

The details of the incident should be sent to the E-Safety Coordinator and include the following information.

Adopted and signed on behalf of the Board of Governors	OCTOBER 2017
Signature of Governor	
Signature of Subject Coordinator / Principal	
Review Date	October 2019