St Patrick's Primary School, Mullinahoe

ICT Acceptable Use Of Internet Policy

Approved by BOG: 30th July 2021

CONTEXT

This policy is based on and complies with DENI Circular 2013/25 on 'eSafety Guidance'. It also complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circular 2011/22 and circular 2016/27 on Internet Safety.

This policy applies to all members of the School community who have access to and are users of the school ICT systems, both in and out of school. This includes pupils, staff including, all teaching and nonteaching staff, the Board of Governors, visitors, volunteers and other individuals who work for or provide services on behalf of the school.

This policy incorporates our Acceptable Use policy. It also must be read in conjunction with other relevant school policies including Data Protection policy, Child Protection policy, UICT policy, Anti-Bully policy and Behaviour policy.
This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in St Patrick's Primary School.

RATIONALE

St Patrick's Primary School believes that e-safety is an essential element of safeguarding children and adults in the digital world when using technology.
We recognise that the internet and information communication technologies are now an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

St Patrick's Primary School recognises its duty to provide the school community with quality internet access to raise educational standards, promote pupil achievement, support professional work of staff and enhance the school's management functions. We recognise our duty to ensure that children are protected from potential harm online.

RISKS

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
- Unauthorised 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

The "Safeguarding Board for Northern Ireland (SBNI); Executive Summary – January 2014" categorises these risks into four main areas:

Content Risks: The child or young person is exposed to harmful material;

Contact Risks: The child or young person participates in adult initiated online activity;

Conduct Risks: The child or young person is a perpetrator or victim in peer-to-peer exchange;

Commercial Risks: The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs.

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 St Patrick's 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.

ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of Child Protection 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) the NSPCC and Childnet.

The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e -Safety throughout the school. The ICT co-ordinator will work closely with the Designated Teacher for Child Protection Mrs Mulholland and Deputy Designated Teachers to promote online safety and address any concerns that may arrise.

The Principal, Mrs O'Hagan and Mr Quinlivan have the responsibility to update Senior Management and Governors with regard to e-Safety and all governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice.

The C2k Network provides robust filtering and security software. Monitoring reports of the use of this Network is available to the Principal/Network Manager on request.

The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community. The Principal ensures that there time alocated in school for monitoring and support for those who carry out the internal online safety monitoring role. The Principal is responsible for ensuring that suitable training is undertaken to enable the school to carry out their online safety roles and to train other colleagues, as relevant.

REVIEWING ONLINE SAFETY POLICY

This policy, supported by the school's 'Acceptable Use Agreements' for staff, governors, visitors and pupils and the 'Staff Code of Conduct' is to protect the interests and safety of the whole school community.
It is linked to other school policies including those for:

- ICT
- Policy for Promoting Positive Behaviour
- Child Protection
- Anti-bullying.

It has been agreed by the Senior Management Team, Staff, parents and pupils and has been ratified and adopted by the Board of Governors.
The Online Safety Policy and its implementation will be reviewed annually.

SAFEGUARDING TEAM

The Safeguarding team is aware of the potential for serious child protection issues to arise from:

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

The member of the Safeguarding team responsible for reporting Online Safety concerns to is Mr Canavan.

NETWORK

The school's technical infrastructure is secure and not open to misuse or malicious attack. The school meets required online safety technical requirements and any EA Online Safety Policy/guidance that may apply. Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. The use of the network/ internet/ email is monitored in order that any misuse/attempted misuse can be reported to the principal/Online Safety Leads/ for investigation.

The school Internet access is filtered through the C2k managed service using a Websense filtering solution. Monitoring systems include robust filtering and security software which is updated as agreed in school policies. Websense assesses all websites based on their content and adds them to a category. (Green - available. Red - unavailable) Monitoring reports of the use of C2k are available on request. All users are given access to a core group of green sites. The school has the facility to customise security options where need arises. Access to the most inappropriate sites will always remain blocked. The school infrastructure and individual workstations are protected by up to date virus software as updated by C2K. (Coordinated updates) Users may only access the networks and devices through a properly enforced password protection policy i.e. passwords are regularly changed. The "administrator" passwords for the school ICT system, used by the Network Managers are kept in a secure place.

HANDLING E-SAFETY ISSUES

Issues of Internet misuse and access to any inappropriate material by any user should be reported to the ICT Co-ordinator to be recorded in the E-Safety log. Issues of a child protection nature will be reported to the designated teacher and dealt with in accordance with the Holy Family Primary School Child Protection Policy. Incidents of pupil misuse of technology which arise will be dealt with in accordance with the school's discipline policy.

ROLE OF STAFF

Teachers are the first line of defence in Online Safety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Incidents will vary from the innocent mistakes to unacceptable behaviour and illegal activity. Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils. Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network. Staff will be encouraged to use the internet to support and enrich their own teaching and professional development. Staff will observe all restrictions and policies with regards to appropriate use of the internet. Any complaint about staff misuse must be referred to the principal. This facility is not for personal use.

- All staff have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices.
- All staff will read, understand and sign annually the staff AUP.
- All staff will report any suspected misuse or problem to principal/ICT/Safeguarding Team for investigation/action/sanction.
- All staff are responsible for ensuring that all digital communications with pupils, parents, carers should be on a prefesslonel level and only carried out using official school systems.
- No filtering service is 100% effective: therefore, all children's use of the Internet is supervised by an adult.
- The use of the Internet is a planned activity. Aimless surfing is not our approach rather children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Children are taught what Internet use is acceptable and what is not.
- Children are 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.
- To ensure children are taught the code of acceptable use.

E-MAIL

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an 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.

Parents/Carers

Parents/carers have an important role to play in promoting Online Safety. We encourage all parents/carers to become involved in Online Safety discussions/in school training and other activities with their child.

- The school continues to share dedicated to Online Safety with links to sites such as CEOP's thinkuknow, Childline, and the Kidsmart page which parents can use with their children.
- The school Twitter account will be used for notifications.
- The school communicates relevant Online Safety information through parents' evenings/newsletters and Twitter account.
- Parents/carers are asked to read through and sign the Acceptable Use Agreement with their child.
- Parents/carers are required to give written consent to images of their child being taken/used.

Parents are reminded regularly that it is important to promote Online Safety in the home and to monitor Internet use.

The following guidelines recommended by the NSPCC are provided.
Parents should:

- 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 online 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 Techno's rules and the SMART tips and promote them at home.
- 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.

Mobile Phones

Mobile phones are brought into school at own risk.
St Patrick's Primary School does not allow the use of mobile phones by children in school or on school trips. The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone.
In these exceptional circumstances, permission must be sought in writing from the Principal. On occasion and when deemed necessary, the class teacher will take charge of the phone during the school day. The use of mobile phones for staff is for personal use only. Mobile phones are switched off or on silent except during non-contact time and at times of personal stress. The principal will have been made aware in confidence by staff when this arises.

It is important to be aware of the safety issues regarding mobile phones which now increasingly have Internet access. Staff use of mobile phones, only when necessary, should be discreet.

When on school outings, teachers are asked to keep their phone on to facilitate contact with school office. First Aiders may also be asked to keep their phones switched on in the event of an emergency.

Staff are advised not to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity unless number is blocked (at staff's discretion).

Staff will have the use of a school land line where contact with pupils or parents is required.

SMART WATCHES

Pupils are not permitted to wear Smart watches with camera/video/audio capabilities.

iPADS

iPads are used for digital storytelling. internet research, and to support learning and teaching across the curriculum via the use of a range of appropriate apps. When using iPads, children will be reminded to be Internet Wise and apply the Internet safety rules. They will not be allowed to use iPads to:

- Take photos of pupils/staff without permission or direction from the teacher .
- Take videos of pupils/staff without permission or direction from the teacher.
- Communicate through any app unless using their own name e.g. Minecraft.

Managing Video-conferencing

Videoconferencing will be via the C2k network to ensure quality of service and security. Any videoconferencing will be appropriately supervised.

Digital Recordings

We record learning and teaching on occasions as a tool to share best teaching practice, celebrate pupil achievement and enhance home/school partnerships. We gain permission to use these from child and parent and adhere to GDPR guidelines to ensure that our practice is fully compliant. Staff or other visitors to St Patrick's should never use a personal device – mobile phone, digital camera or other digital recording device to take photographs, video or sound recordings of the pupils.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission, except where disclosed to the Police as part of a criminal investigation.

Use of Images, Video and Sound

It is recognised that many aspects of the Curriculum are enhanced by the use of multimedia. Staff and Pupils at St Patrick's Primary School are encouraged to use iPads to create and use digital images, videos and sound recordings. They are taught to do so in a safe and responsible manner. Digital images, video and sound recordings are only taken with the permission of the participants. Images and video are of appropriate activities and full names of participants are not used. Parents/carers are required to sign an agreement annually regarding the taking and publishing of digital images of their children. This consent form is considered valid for the entire school year 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 wilt not enable individual pupils to be clearly identified by name.

Storage of Images

Digital and video images of pupils are always taken using school devices. Images are only permitted to be stored on a centralised area on the school network and are accessible to staff and to pupils under supervision. Photographs of pupils are generally removed when they leave school. Written permission from parents or carers will be obtained before photographs/videos of pupils are published on the school and third party websites.

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 Online Safety rules. These Online Safety rules will also be displayed clearly in all rooms.
- All parents/guardians will be asked annually to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's Online Safety rules policies.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Handling Online Safety Complaints or Misuse

- Complaints of Internet misuse will be dealt with by a senior member of staff. If deemed necessary PSNI education partners may become involved.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the Online Safety incident logbook (kept securely in the main office).
- As port of the Acceptable Use Agreement children will know that if they deliberately break the rules they could be stopped from using the Internet/E-mail and that parents/carers will be informed.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

Cyberbullying

Cyberbullying can take many forms and guises including:

- **E-mail** – nasty 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 the sharing of 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 else.

Incidents of cyber-bullying will be dealt with in accordance with the School Anti-Bullying Policy.

Our Five Key Principles

To ensure responsible use and the safety of pupils the school's policy is built on following five key principles:

1. **Guided educational use.**

No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult. Internet use will be planned, task orientated and educational within a regulated and managed environment. 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.

2. **Risk assessment.**

Both staff and pupils will be aware of the risks associated with Internet use. Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.

3. **Responsibility.**

Internet safety depends on staff, governors, advisors, parents, and, where appropriate, pupils themselves taking responsibility for use of the Internet and associated technologies. The school will seek to balance education for responsible use, regulation and technical solutions to ensure pupils' safety.

4. **Regulation.**

The use of the Internet, which brings with it the possibility of misuse, will be regulated. Fair rules will be agreed for pupils to discuss and understand, they will be prominently displayed as a constant reminder of the expectations regarding Internet use.

5. **Appropriate Strategies.**

Effective, monitored strategies will be in place to ensure responsible and safe Internet use. The school will work in partnership with the Department of Education, parents and C2k to ensure systems to protect pupils are regularly reviewed and improved. Access to the Internet is provided through a filtered service, this C2k managed service is designed to filter out unsuitable material.

Points for Children to Consider

Follow These SMART TIPS

Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!

Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committees

Acceptable Use of the Internet

We believe that all users should have an entitlement to safe Internet access at all times. As such, this Acceptable Use Policy is intended to ensure that:-

- ✓ All staff and pupils will be responsible users and stay safe while using the Internet and other communications
- ✓ All staff and pupils will adhere to Password security guidelines as stated in the e-safety policy
- ✓ All staff and pupils are familiar with acceptable and unacceptable internet use.
- ✓ Acceptable use of internet for both pupils and staff covers both fixed and mobile internet technologies provided by school as well as those owned by pupils and staff but brought onto school premises.
- ✓ All staff have read, understood and signed the school's Staff Acceptable Use Policy. *
- ✓ New staff members will receive a copy of the e-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.*
- ✓ The Acceptable Use Agreement will also apply to external agencies/facilitators who, for reasons of staff training or presentation to pupils and parents, make use of the school's ICT equipment. *

The following rules apply to all pupils:

St Patrick's Mullinahoe Code of Acceptable Use

- *I will only access the system through my proper log-in and will keep any passwords secret;*
- *I will not access other people's files;*
- *I will only use the school computers/iPad's and other devices for school work and homework;*
- *I will not bring MP3's, USB's mobile phones or other mobile storage devices from outside school unless I have been given permission by my teacher;*
- *I will always ask permission from a member of staff before using the internet;*
- *I will only email people my teacher has approved;*
- *The messages I send will be polite and responsible and checked by my teacher;*
- *I will never give my home address, telephone number, or arrange to meet someone;*
- *I will report any unpleasant material or messages sent to me to my teacher. I understand this report would be confidential and would help protect other pupils;*
- *I understand that the school may check my computer files and may monitor the Internet sites I visit;*
- *I understand that if I deliberately break these rules I could be stopped from using the Internet;*

Policy Review

Internet technology and school use of resources will develop and change with time. It is our intention to revise and up-date our Internet Safety Policy as appropriate and where necessary. The school is preparing for an C2k update this school year 2018/19. A programme of work will take place between April and the end of June this year to transition all compatible devices to Windows 10 in Primary, Special and EOTAS centres.

This update, changes to GDPR and the new Bullying legislation will need to be reflected in our updated policy which will be reviewed as soon as our C2k update is completed and further ramifications are clear.

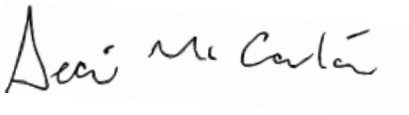
Parents are required to sign and return the form attached **acknowledging their understanding of the school's policy and Code of acceptable use on Internet use**.

Guidance Material on Internet Safety
http://schoolsl.becta.org.uk
www.ceop.gov.uk
www.thinkuknow.co.uk

Examples of safety rules for children are also available from:
http://www.kented.org.uk/ngfl/policy

Head Teacher (J Canavan) **Chair of Governors (Fr S McCartan)**

Signed: 

Signed: 

Date: 6- 10 -16

Date: 6- 10 -16

Acceptable Use Agreement for Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- All Internet activity should be appropriate to staff professional activity or the pupils' education
- Access should only be made via the authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

Name; _____

Signed; _____

Date; _____

St Patrick's Mullinahoe
ICT Suite Code of Conduct

Our Pupil Council have worked hard to devise this code of contact after meeting with staff and KS1 and KS2 classes. We would ask that you please abide by the following rules whilst in the ICT suite and by the rules in the Acceptable Use Agreements and Internet Usage Policy. St Patrick's Primary School Mullinahoe uses internet monitoring and filtering tools.

General

- Do not enter the ICT Suite without staff permission
- Students should be aware that school staff can see your actions on the network, when using the Internet or E-mail
- Do not eat or drink any food in the ICT Suite
- Do not have any food or drink in the ICT room
- Do not bring any personnel electronic devices (Mobile Phones, MP3 players, etc) into the ICT room
- Behave appropriately at all times
- Students must NOT give their password to anyone else
- Students must NOT use someone else's user accounts including loging on to the network for anybody else
- Students must NEVER communicate your own or any other pupil's personal details via E-mail or on any internet sites
- Students must NOT use or send inappropriate language.
- Never arrange to meet anybody who may approach you via E-mail or on a website/chat room; they may not be who they say they are
- Inappropriate material in a user area is the user area owner's responsibility/fault
- Do not use speakers or headphones without permission
- Do not use the USB /DVD drives without permission
- Do not 'LOGON' until asked to do so by your teacher
- Strictly follow the rules and responsibilities in the Acceptable Usage Agreement and Internet Usage Policy
- Students should sit in their allocated seat
- Students must NOT waste resources, this includes paper, ink, internet access and lesson time by misusing ICT resources
- Respect the ICT rooms and equipment that are provided by the school for your use. Report any problems to a member of staff.
- Students will be held accountable for any poor or irresponsible behaviour that results in damage to any of the ICT equipment. In such cases the cost of repairs or replacement of equipment will be requested from the student's parent or guardian.

Rules relating to the Internet

When using the Internet, you must NOT....

- Play online games (unless asked to do so by your teacher)
- Use games sites, chat rooms, forward chain mails, download music and/or video clips and use mobile phone sites.
- Download and/or install any unauthorised games or application software onto any school computer.
- Use 'Chat Lines' or messenger software
- Download or install any program files
- Fill in forms or give personal details out
- Use or access inappropriate web sites
- Send, access or display offensive messages, pictures or audio/video files
- Communicate using inappropriate language

The school reserves the right to administer these rules in a fair and unbiased way, which may result in a student's access to either the internet or the school network being removed or other appropriate sanction being taken.