St. Eugene's P S
Derry

"Do My Best"

e Safety Policy
1. INTRODUCTION

“E-safety or electronic safety is about utilising electronic devices or e-technologies in a safe and responsible way. It is mainly concerned with the safeguarding of children and young people in the digital world and educating them so they feel safe when accessing e-technologies.” [NCB NI definition]

The term internet safety and e-safety are often used interchangeably. However, the term internet safety implies that it is just about the internet and computers, whereas e-safety includes all devices which have an online connection such as mobile phones, games consoles, cameras and televisions.

‘Online safety, in all cases, in schools and elsewhere, remains a paramount concern. Schools play a crucial role in raising awareness of the risks, highlighting the impact of behaviour when engaging with online technologies and educating children and young people about how to act appropriately and stay safe.’ DENI 2016/27

St Eugene’s Primary School recognises that ICT and the internet are essential tools for learning and communication in the 21 century. They can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practise good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

We are aware that some adults and young people will use these technologies to harm children, from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a ‘duty of care’ for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty.

It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy strives to ensure that St. Eugene’s P S is working to safeguard and promote the welfare of its pupils. E-Safety is a safeguarding issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required
procedures and to act on them. It aims to put into place effective management systems and arrangements which will maximise the educational benefit whilst minimising any associated risks. It describes actions to redress any concerns about child welfare and safety as well as how to protect our pupils and staff from risks.

"It is essential that pupils and adults are kept safe online whilst in school and on school-organised activities. Schools have a responsibility to ensure that there is a reduced risk of pupils accessing harmful and inappropriate digital content. Schools should be energetic in teaching pupils how to act responsibly and keep themselves safe in the digital world and as a result, pupils should have a clear understanding of online safety issues and be able to demonstrate what a positive digital footprint might look like for themselves." DENi 2016/27

The whole school community has the responsibility for safeguarding and promoting the welfare of pupils in their care. The Principal will co-ordinate with the Safe guarding team, the Board of Governors and the ICT co-ordinator to ensure our policy is compliant with good child protection practices.

This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use and as a reference for their conduct online during and outside of school hours. E-safety is a whole- school issue and responsibility. This document sets out the policy and practices for the safe and effective use of the 'Internet' in School. The policy has been drawn up in consultation with the staff, safe guarding team and ICT Coordinator. It has been approved by the Board of Governors and is available to all parents if requested. Articles 17, 18 and 19 of the Education and Libraries (Northern Ireland) Order 2003 place a statutory duty on Boards of Governors (BoG) to safeguard and promote the welfare of its pupils and to determine the measures to be taken at the school with a view to protecting pupils from abuse (whether at school or elsewhere).

It is also the duty of the Board of Governors to determine the measures to be taken in a school to protect pupils from abuse (Article 18 of the Education and Libraries (Northern Ireland) Order 2003). In the exercise of those duties, Boards of Governors must ensure that their schools have a policy on the safe, healthy, acceptable and effective use of the Internet and other digital technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils which will serve to reassure parents. This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are
displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PDMU lessons where personal safety, responsibility, and/or development are being discussed.

This e-safety policy relates to the use of the internet, use of mobile phones and use of digital/photographic images of children. It is based largely on DENI Circulars 2007/1, 2013/25 and 2016/26 "Acceptable Use of the Internet and Digital Technologies in Schools" and should also be read in conjunction with the School’s Child Protection Policy, Photographic policy and Mobile Phone policy, Code of Practice and Anti-bullying policy. In January 2014, the SBNI published its Report ‘An exploration of e-safety messages to young people, parents and practitioners in Northern Ireland’. The report points to important factors which should be taken into account, not least that young peoples’ extensive use of technology leaves no doubt over the importance of online safety.

Children and young people have a right to be protected and educated. The report highlights the requirement to take appropriate preventative action to protect children and minimise the associated risks around online safety. These risks have been defined under four categories:

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

**Contact risks**: The child or young person participates in adult-initiated online activity and/or is at risk of grooming.

**Conduct risks**: The child or young person is a perpetrator or subject to bullying behaviour in peer-to-peer exchange and/or is at risk of bullying, entrapment and/or blackmail.

**Commercial risks**: The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs/fraud.

**C2K**

C2K supports the implementation and sharing of effective practices and collaborative networking across the Province, as well as nationally and internationally. Staff will be encouraged to use C2K resources in their teaching and learning activities. Electronic information-handling skills are fundamental to the preparation of pupils for employment in the 'Information Age.' Staff will be encouraged to investigate the possibilities provided by access to this electronic information and communication resource and blend its use, as appropriate, within the curriculum. They should model appropriate and effective use and provide guidance and instruction to pupils in the acceptable use of the Internet. C2k is responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.
Some of these safety services include:

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

In addition to the above
C2k provide the following to facilitate the process of safeguarding children.

Filtering
Filtering on the C2k network is grouped as follows:
Internet Advanced - allowing access to a wider range of pages than the default including webmail, shopping, drugs and alcohol, sex education.
Internet Streaming - allowing access to streaming media websites including Youtube, BBC iPlayer, TV and radio streaming sites. (when permitted)
Internet Social Networking - allowing access to social networking sites including Facebook, Twitter, (when permitted)
C2k, through the managed service provider, adhere to ISO 27001 standard security around the C2k EnNI system:
Forcepoint (formally Websense) filtering in place for Internet access.
Nightly Internet Watch Foundation (IWF) updates.

Option to sign up to Delegated Access. This provides the school with more control over their own Internet filtering. Inappropriate websites remain blocked. Delegated access offers schools the facility to report on internet usage without going through the Service Desk.

All staff and student/pupil internal and external email is filtered for inappropriate content. Should the school decide to access online services through service providers other than C2k then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.
2. INTERNET SAFETY

The Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life and our school provides pupils with opportunities to use resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools." DENI circular 2007/01

The purpose of internet use in school is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the school’s management and administration system. The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide pupils with quality access as part of their learning experience.

Technology is now a huge part of all aspects of everyday life, education and business. We want to equip our pupils with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

It is also important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Pupils will be taught to use age-appropriate tools to search for information online and to acknowledge the source used and to understand the concept of respecting copyright.

The school will also take steps to filter internet content (C2K) to ensure that it is appropriate to the age and maturity of pupils. Teachers will ensure any proposed search will not result in the access of inappropriate material. If staff or pupils discover unsuitable sites then the URL will be reported to the Principal, ICT co-ordinator, Designated or Deputy Designated teacher. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.
ICT brings benefits for all the school community:

Benefits for teachers

With countless online resources, technology can help improve teaching. Teachers can use different apps or trusted online resources to enhance the traditional ways of teaching and to keep pupils more engaged. Virtual lesson plans, online assessments can help teachers. What is more, having virtual learning environments in schools enhances collaboration and knowledge sharing between teachers.

• Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.

• Immediate professional and personal support through networks and associations.

• Improved access to technical support.

• Ability to provide immediate feedback to pupils and parents.

• Class management, attendance records, schedule, and assignment tracking.

For students:

• Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.

• Contact with other schools resulting in cultural exchanges between pupils.

• Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.

• An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.

• Access to learning whenever and wherever convenient.

• Freedom to be creative.

• Freedom to explore the world and its cultures from within a classroom.

• Social inclusion, in class and online.

• Access to case studies, videos and interactive media to enhance understanding.

• Individualised access to learning.
Teaching and Learning advantages using ICT and the internet in schools are:

Improves engagement with different opportunities to make learning more enjoyable

Improves knowledge retention as pupils who are engaged and interested will recall what they have done better.

Encourages individual learning with technology providing great opportunities for making learning more effective for everyone with different with learning styles, different abilities and needs.

Encourages collaboration with pupils in the same classroom, same school and even with other classrooms around the world.

Learn useful life skills by collaborating with others, solving complex problems, critical thinking, developing different forms of communication and leadership skills, and improving motivation and productivity.

For parents:

(Teachers2parents) allows for the communication of messages to parents via text messaging service

(Facebook) similarly allows for the posting of messages to parents and the opportunity for parents to make enquiries from the school.

(Website) allows for school events and school documentation to be made available to parents.

3. ETHOS

Safeguarding and promoting the welfare of pupils is paramount in the ethos, practice and procedures of St. Eugene’s P S. All staff have a responsibility to support e-Safety practices in school and all pupils need to understand their responsibilities if there are deliberate attempts to breach e-safety rules. It is the duty of the school to ensure the safety of every child in its care and the general principles of such also apply to any community organisations etc that make use of the school's ICT facilities.

Cyber Bullying

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying should be considered within the school’s overall anti-bullying policy and pastoral services as well as the e-Safety policy. Care should be taken when making use of social media for teaching and learning. Each of the social media technologies can offer much to schools
and pupils but each brings its own unique issues and concerns. Each social media technology that is to be utilised should be risk assessed in the context of each school situation.

*(Social media interactions do not form any part of the general teaching and learning ICT environment within St. Eugene’s PS and such use would only be considered as part of a specific project which would need to be agreed, risk assessed and done through the school computers and overseen by school staff)*

Cyber Bullying can take many different forms and guises including: nasty or abusive emails, 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 can also occur 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 and pupils should be reminded that cyber-bullying can constitute a criminal offence.’ *(DENi 2013/25)*

Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school’s Anti-Bullying Policy.

It is important that pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

St Eugene’s primary School will record cyber-bullying incidents if they are reported to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions. Complaints related to child protection will be dealt with in accordance with the school’s Safeguarding/Child Protection Policy.
4. ROLES AND RESPONSIBILITIES

The Principal will ensure that:

All staff are included in e-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal. The ICT co-ordinator will receive appropriate training, support to deal with safeguarding issues. All staff including temporary and volunteers will be made aware of the school’s e-Learning/Safety Policy and arrangements.

The Governing Body of the school will ensure that:

The Principal or a member of the school’s leadership team is designated to take the lead on e-Learning/Safety within the school. Procedures are in place for dealing with breaches of e-safety and security and are in line with EA procedures. All staff have access to appropriate ICT training.

The Principal or Designated Senior Member of Staff for e-Learning/Safety will:

Act as the first point of contact with regards to breaches in e-safety / security. Liaise with the Designated Teacher for Safeguarding as appropriate. Ensure that ICT security is maintained. Attend appropriate training and provide support and training for staff and volunteers on e-Safety. Ensure all staff are aware of the school’s e-Learning/Safety Policy. Ensure that the school’s ICT systems are regularly reviewed with regard to security. Ensure that the virus protection is regularly reviewed and updated and that staff take responsibility for keeping their laptops up to date.

Staff and Pupils on the Internet

When using the Internet, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws and all school staff (both teachers and support staff) are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector. Pupils are responsible for their good behaviour on the school networks. While the issue of information and communication technologies is a required aspect of the statutory Northern Ireland Curriculum, access to the Internet and to C2K remains a privilege and not a right. It is given to pupils who act in a considerate and responsible manner and will be withdrawn if they fail to maintain acceptable standards of use.
Staff will ensure pupils know and understand that no Internet user is permitted to:

- retrieve, send, copy or display offensive messages or pictures;
- use obscene or racist language;
- harass, insult or attack others;
- damage computers, computer systems or computer networks;
- violate copyright laws;
- use another user's password to gain access to the computer network.
- trespass in another user's folders, work or files;
- intentionally waste resources (such as on-line time and consumables);
- use the network for unapproved commercial purposes.

Use of the C2K services by St. Eugene's P.S. must be in support of the aims and objectives of the Northern Ireland Curriculum.

4 TEACHING and LEARNING

Benefits of internet use for education

The internet is a necessary tool in the delivery of the statutory curriculum and a for staff and children and benefits education by allowing access to world - wide educational resources. Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the pupils.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be taught research techniques including the use of search engines. Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work if appropriate.

Access to the internet supports educational development and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home. The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of resources and administration data with C2k, DENI and EA.
5 EXAMPLES OF ACCEPTABLE AND UNACCEPTABLE USE.

On-line activities which are encouraged include, for example

- the use of e-mail and computer conferencing for communication between colleagues, between teacher(s) and teacher(s), between pupil(s) and pupil(s), between schools and industry; (supervised)
- use of the Internet to investigate and research school subjects, cross curricular themes and topics related to social and personal development;
- the development of pupils' competence in ICT skills and their general research skills;

On line activities which are not permitted include, for example:
- searching, viewing and/or retrieving materials which are not related to the curriculum.
- copying, saving and/or redistributing copyright protected material, without approval;
- playing computer games or using other interactive 'chat' sites, unless specifically assigned by the teacher;
- publishing, sharing or distributing any personal information about a user (such as; home address; e-mail address; phone number, etc.);
- any activity which violates a school rule.

6 LOCATION AND SUPERVISION

The school will ensure that access to the Internet provided to Staff and pupils through any Internet Service Provider is a filtered service. All users will be aware that the school can and will track and record the sites visited, the searches made on the Internet and the e-mail sent and received by individual users.

Internet access for pupils in the school will be available only on computers in the computer suite and classrooms. Machines which are connected to the Internet will be in full view of people circulating in those areas. While using the Internet at school, pupils will be supervised at all times. The school will ensure that all pupils understand how they are to use the Internet appropriately and why rules exist. The ICT Co-ordinator may review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored on C2K servers to be absolutely private.
7 MANAGING INTERNET ACCESS

Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.

Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator.

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

Pupils will be taught to be critically aware of the materials they read.

8 MANAGING e-MAIL

Personal e-mail or messaging between staff and pupils should not take place.

Staff must use the school e-mail address if they need to communicate with pupils about their school work e.g. homework etc. (Not applicable in St. Eugene’s PS)

Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail. Whole class or group e-mail addresses should be used. (Pupils do not have individual e-mail accounts)

Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone. (Pupils do not use an e-mail facility in St. Eugene’s PS)

Access in school to external personal e-mail accounts may be blocked.

E-mail should be authorised before sending to an external organisation just as a letter written on school headed note-paper would be.

Incoming e-mail should be monitored and attachments should not be opened unless the author is known.
Emails

The school uses email internally and externally for staff only and is an essential part of school communication.

It may be used (with the Principal / ICT co-ordinators permission) to enhance the curriculum by initiating contact and projects with other schools nationally and internationally.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to. Primary schools should only have whole class emails or project email address.

E-mail policy

- Staff should **not** use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should **not** be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

**MANAGING WEBSITE CONTENT**

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only.
Colour photographs and pupils work bring our school to life, showcase our student’s talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material. The Principal is ultimately responsible for all information placed on the website. Permission may be granted to others on staff to post information provided they follow the safety guidelines agreed. Pupils names should not accompany their photograph and only those photographs of pupils whose parents have given signed permission can be placed on the website.

Editorial guidance will ensure that the school’s ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

Photographs of pupils will not be used without the written consent of the pupil’s parents/carers. (Written permission for the use of photographs on St. Eugene’s PS website and or Facebook will be sought.) The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil’s home information will not be published.

The Principal or nominated person(s) will have overall editorial responsibility and ensure that all content is accurate and appropriate. The website will comply with the school’s guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing. Use of site photographs will be carefully selected so that pupils cannot be identified or their image misused.

Pupils’ names will not be used on the website, particularly in association with photos. Work will only be used on the website with the permission of the pupil and their parents. The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Using photographs of individual children
Photographic permissions policy
Under Data Protection images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school.
The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school’s policy on the use of photographs of children, including:

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place. It is important that published images do not identify pupils or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school’s permission. The school follows general rules on the use of photographs of individual children:

Parental consent must be obtained. Consent will cover the use of images in:
- all school publications
- on the school website
- in newspapers as allowed by the school
- in videos made by the school or in class for school projects.

Electronic and paper images will be stored securely.
Names of stored photographic files will not identify the child.
Images will be carefully chosen to ensure that they do not pose a risk of misuse.

This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities, never taken under any circumstances).

- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the pupils such as school plays or sports days must be used for personal use only. (parents are informed of this prior to every assembly / play)
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.
For more information on safeguarding in school please refer to our school Child Protection and Safeguarding policy and Photographic policy

Complaints of misuse of photographs or video

Parents are unable to post information on the website and the school does not contact parents by e-mail.

10 SOCIAL NETWORKING AND CHAT ROOMS

The school will control access to moderated social networking sites and educate pupils in their safe use. (Pupils engagement in chat rooms etc will be project specific, closed with regard to engagement and only engaged in under teacher’s supervision.)

Pupils will not access social networking sites e.g. ‘Facebook’.

Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.

Pupils will not be allowed to access public or unregulated chat rooms from school.

Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of the Principal or senior management should always be sought first and language should always be appropriate and professional.

11 MOBILE PHONES

Mobile phones and personal device

While mobile phones and personal communication devices are commonplace their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

➢ they can make pupils and staff more vulnerable to cyberbullying
➢ they can be used to access inappropriate internet material
➢ they can be a distraction in the classroom
➢ they are valuable items that could be stolen, damaged, or lost
➢ they can have integrated cameras, which can lead to child protection, bullying
➢ and data protection issues.
The school takes certain measures to ensure that mobile phones are not used irresponsibly in school. In St Eugene’s PS the general rule is that phones should be ‘not seen and not heard.’ Any child who brings a phone to school and it becomes known to the teacher will have the phone taken as a matter of security and returned at the end of the day. Phones as such cannot be banned as some pupils claim that they need the phone to contact parents after school.

If it is found that a phone has been used inappropriately
• The school will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school’s disciplinary sanctions read the **Positive behaviour policy**.

• Mobile phones can be confiscated by a member of staff if there is reason to believe that there may be evidence of harmful or inappropriate use on the device. Parents will be asked to come to the school and it is they who will search the phone records.
• Mobile phones must be switched off during school lessons or any other formal school activities.
• Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.

• Images or files should not be sent between mobile phones in school.

• Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school’s positive behaviour policy. Their mobile phone may be confiscated before being returned to a parent. *(see Mobile phone policy)*

**Staff**
• Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
• Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
• The school expects staff to lead by example. Personal mobile phones should be switched off or on ‘silent’ during school hours. *(permission may be sought from the Principal for exemption if there is a genuine personal need)*
• Any serious breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the **child protection and safeguarding policy**, or in the staff contract of employment.
Mobile phones will not be used during lessons or formal times in school. The sending of abusive or inappropriate text messages or files is forbidden and will be dealt with in accordance with the school’s Anti-Bullying and Behaviour Policies.

Use of cameras in their mobile phones by pupils will be kept under review and only for specific educational purposes. St. Eugene’s Primary School Mobile phone policy works on the premise that they should be ‘not seen and not heard.’ Staff will be issued with a school mobile phone where contact with pupils is necessary or where mobile phones are used to photograph school activities involving pupils.

11 FILTERING

The school will work in partnership with parents/carers, the Education Authority, DENI and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported and the e-Safety Co-ordinator / Principal.

Any material the school deems to be unsuitable or illegal will be immediately reviewed.

Regular checks by Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

Filtering methods will be selected by the school in conjunction with C2k and will be age and curriculum appropriate.

12 AUTHORISING INTERNET ACCESS

All staff must read the school’s ‘Code of Conduct for ICT’ before using any ICT resources and any staff not directly employed by the school will be asked to sign the school’s ‘Acceptable Use of ICT Resources’ document before being allowed internet access from the school site.

The school will maintain a current record of all staff and pupils who are allowed access to the school’s ICT systems. If parents/carers have specifically requested that their child be denied internet access the school will maintain a record of this.

Parents/carers will be informed of the school’s ‘Acceptable Use’ document and given a copy upon request. Permission for their child to access ICT resources is taken as given unless the school is informed otherwise.

Staff will supervise access to the internet from the school site for all pupils.
13 PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

When not in use all video conferencing cameras will be switched off.

It is not appropriate to use photographic or video technology in changing rooms or toilets. Staff may use photographic or video technology to capture to support school trips and appropriate curriculum activities. Audio and video files may not be downloaded without the prior permission of the teacher. Pupils will be supervised when making or answering a videoconference call or making a video or audio recording in school or on educational activities. Videoconferencing and webcam use will be appropriately supervised for the pupil’s age.

14 ASSESSING RISKS

Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Education Authority can accept liability for the material accessed, or any consequences of Internet access.

Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

The Principal / designated teacher / deputy designated teacher will ensure that the e-Safety Policy is implemented and compliance with the policy is monitored.
14  INTRODUCING THE POLICY TO PUPILS

Rules for Internet access will be posted in all rooms where computers are used.

Responsible Internet use, covering both school and home use, will be included in the curriculum. Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet and that internet use will be closely monitored and that misuse will be dealt with appropriately.

15  CONSULTING STAFF

It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

All staff are governed by the terms of the school’s ‘Staff Code of Conduct for ICT’ and will be provided with a copy of the e-Safety policy and its importance explained. All new staff will be given a copy of the policy during their induction. Staff development in safe and responsible use of the internet will be provided as required. Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential. Senior managers will supervise members of staff who operate the monitoring procedures.

16  MAINTAINING ICT SECURITY

ICT systems will be monitored through C2K. All planned ICT activities will take place under the supervision of school staff. Staff passwords will not be freely available or shared with pupils. Passwords will be changed in accordance with C2K procedures.

17  DEALING WITH COMPLAINTS

Pupils and parents/carers will be informed of the complaints procedure.

Staff, Pupils, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures.

The Principal or the school’s designated or deputy designated teacher will deal with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Principal immediately. Parents/carers and pupils will work in partnership with the school staff to resolve any issues.
There may be extreme incidents when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

Sanctions for misuse may include any or all of the following:

- Interview/counselling by appropriate staff, pupils will not be alone.
- Informing parents/carers.
- Removal of internet access for a specified period of time, which may ultimately prevent access to files, held on the system, including examination coursework.
- Referral to the police.

18 PARENTS/CARERS SUPPORT

Parents will be informed of the school’s e-safety policy which may be accessed on the school website or requested from the school office. Any issues concerning the internet will be handled sensitively to inform parents/careers without undue alarm.

Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.

Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

A partnership approach will be encouraged with parents and this may include practical sessions as well as suggestions for safe internet use at home.

19 ADVICE FOR PARENTS

While in school, teachers will guide pupils towards appropriate materials on the Internet. Outside school, parents or guardians bear the same responsibility for such guidance as they would normally exercise with information sources such as television, telephones, movies, radio and other media.

Appropriate home use of the Internet by children can be educationally beneficial and can make a useful contribution to home and school work. It should, however, be supervised and parents should be aware that they are responsible for their children’s use of the Internet resources at home.

It is good practice that parents provide filtered and monitored access to the Internet and consider any appropriate guidance and advice on its use that they might find helpful at home.
Such guidance and advice will include the following:

- parents should discuss with their children the rules for using the Internet and decide together when, how long, and what comprises appropriate use;
- parents should get to know the sites their children visit and talk to them about what they are learning;
- 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 a credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud;
- parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images.

If the message comes from an Internet service connection provided by the school or C2K, they should immediately inform the school.

**Code of Safe Practice**

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. We have a Code of Safe Practice for pupils (Appendix) and staff (Appendix) 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, and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, camera phones, PDAs) is subject to the same requirements as technology provided by the school.

The ICT co-coordinator and the Principal will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology. ICT resources may be increasingly used as part of the Extended school agenda and as such external adult users will sign the school’s acceptable use policy.
**Code of Safe Practice for Pupils**

The code of practice for pupils will be made known to parents at the beginning of each year and their consent taken as given unless the school is informed otherwise.

In addition, the following key measures have been adopted by St. Eugene’s PS to ensure our 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 and e-Safety guidelines are displayed prominently throughout the school;

Our Code of Practice is reviewed regularly and made known to pupils/parents when required:

- Pupils using the Internet will work in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and is supervised, where possible;
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group;
- Pupils in Key Stage 2 are educated in the safe and effective use of the Internet, through a number of selected websites.

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

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

**Sanctions**

Incidents of technology misuse which arise will be dealt with in accordance with the school’s Positive discipline and Behaviour Policy. Minor incidents will be dealt with by the Principal and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school’s child protection policy.
**Code of Practice for Staff**

The following Code of Safe Practice has been agreed with staff:

Pupils accessing the Internet should 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.

All pupils using the Internet have permission from their parents unless the school is informed otherwise.

Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal / ICT Coordinator.

In the interests of system security staff passwords should only be shared with the network manager.

Teachers are aware that the C2K system can track 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 a school camera and images should be stored on a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work. (see Digital/Photographic Images Policy)

School systems may not be used for un-authorised commercial transactions.

**Internet Safety Awareness**

In St. Eugene's P S we believe that, alongside having a written e-Safety policy and code of practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.
Internet Safety Awareness for pupils

Rules for the Acceptable Use of the Internet are discussed with all pupils and are prominently displayed in classrooms. In addition, Key Stage 2 pupils are made aware and discuss Internet Safety through structured lessons. There are various pupil resources available such as:

ThinkUKnow KidSMART
Go CBBC
Learning with your child
Know IT All for Schools
NSPCC online safety

Internet Safety Awareness for staff

The ICT Coordinator keeps informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of this policy and strategy on ICT use in teaching and learning and updated in relation to relevant changes. Teachers can download lesson plans, teaching activities and pupils’ worksheets by registering with the Thinkuknow website.

Internet Safety Awareness for parents

The Internet Safety Policy and Code of safe Practice for pupils is made known to pupils and parents at the start of each school year. Additional advice for parents with internet access at home also accompanies this information or Internet safety leaflets for parents also distributed when available.

Health and Safety

In St. Eugene’s P S we have attempted to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the ICT suite. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used. Guidance is also issued to pupils in relation to the safe use of computers. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are also mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.
**Wireless Networks**

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment.

**School Web Site**

The school web site is used to celebrate pupils’ work, promote the school and provide information. Editorial guidance will ensure that the Web site reflects the school’s ethos that information is accurate and well-presented and that personal security is not compromised. As the school’s Web site can be accessed by anyone on the Internet, the school has to be very careful to safeguard the interests of its pupils and staff. The following rules apply. The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils’ home information will not be published.

Web site photographs that include pupils will be selected carefully. Written permission from parents will be obtained before photographs of pupils are published on the school Web site (see Digital Images policy section). Pupils’ full names will not be used anywhere on the Web site, particularly in association with photographs.

The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The Web site should comply with the school’s guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

**Social Software**

**Social networking, social media and personal publishing**

This is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks and blogs (personal web journals). Social environments enable any community to share resources and ideas amongst users. Such software allows users to exchange resources, ideas, pictures and video. The majority of activity in these on-line social sites usually causes no concern. C2k filters out these social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment. Concerns in relation to inappropriate activities would tend to come from use outside the school environment. We regard the education of pupils on the safe and responsible use of social software as vitally important and this is
addressed through our Internet Safety Education for pupils. Appropriate information and indeed education will also be provided for our parents.

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online.

**Pupils are not allowed to access social media sites in school. There are various restrictions on the use of these sites in school that apply staff.**

Social media sites have many benefits for both personal use and professional learning; however, both staff and pupils should be aware of how they present themselves online. Pupils are taught through the ICT curriculum and PDMU about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school’s code of conduct regarding the use of ICT and technologies and behaviour online.

- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe.

- **Official school blogs created by staff or pupils/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.**

- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school and must act appropriately.

- Safe and professional behaviour of staff online will be discussed at staff induction.

Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school’s discipline policy and child protection procedures.

Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.
FURTHER SUPPORT & ADVICE
Further documentation, links to the 360 degree safe website, online safety template and sample acceptable use agreements can be found in the Online Safety area in Fronter.

The Department’s webpage on online safety provides further advice and links to relevant DE Circulars sites providing advice for pupils, parents and teachers.
education-ni.gov.uk/keeping-children-safe-online

The Education Authority Safeguarding site provides useful information on all aspects of safeguarding and child protection:
www.eani.org.uk/schools/safeguarding-and-child-protection/

Adopted by the Governing Body on _________________________

Signed _____________________________ Principal

Signed _____________________________ Chairperson
Primary e-Safety Rules

I will only use ICT in school for school purposes.

I will only use my class e-mail address or my own school e-mail address, (if provided) and open e-mail attachments from people I know, or whom my teacher has approved.

I will not send anyone material that could be considered threatening, bullying, offensive or illegal.

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

I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety

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 give out my own details such as my name, phone number or home address.
I will not arrange to meet someone and I will inform my teacher or parent if anyone asks to meet me.

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

Code of Practice for Staff

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 the Principal.

The following Code of Safe Practice has been agreed with staff:

**Working with pupils**

Pupils accessing the Internet should 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.

All pupils using the Internet have permission from their parents unless the school is informed otherwise.

Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal / ICT Coordinator.

Teachers are aware that the C2K system can track 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.

Images of pupils and/or staff will only be taken, stored and used for professional purposes in line 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, member of staff or Principal.

Photographs of pupils should, where possible, be taken with a school camera and images should be stored on a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work. (see Digital/Photographic Images Policy) School systems may not be used for un-authorised commercial transactions.

**Personal declaration**

I will only use the school’s email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.

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

I will ensure that all electronic communications with staff are compatible with my professional role.

I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.

I will only use the approved, C2k, secure e-mail system for any school business.

I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or BOG. Personal or sensitive data taken off site must be encrypted.

I will not install any hardware of software without permission of Principal.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Principal.
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.

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 to support the safe and secure use of ICT.  

Signature........................................................................................................ Date ............

**Parental Agreement/Consent**

Dear Parent / Carer

E Safety & Internet Usage Policy

September 2018

Letter sent home to all pupils and their parents of KS2. KS1 will have same letter but with their Acceptable Use Agreement

Dear Parents

In school we have access to the internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. At St Eugene’s PS we are aware that young people should have an entitlement to safe internet access at all times. However, school and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

We strongly recommend that children do not use social network sites such as Facebook, Instagram, Snapchat or have YouTube accounts at home. These carry an age-restriction of 13 years old and pose a risk to children. Social networks have no place in our school and so school staff should not be approached by pupils or parents online or invited to join.

Your child has read the following Acceptable Use Agreement (*below*) in class with their teacher. Once they have fully understood them all, your child has signed their name to agree to stick by them. Please read them again at home with your child to show your support of the school in this important aspect of our work. Thank you.
As part of St. Eugene’s Primary School Information and Communications Technology programme we offer pupils supervised access to a filtered Internet service provided by C2k. Access to the Internet will enable pupils to explore and make appropriate use of many web sites 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 provider C2k has installed filtering software which operates by blocking thousands of inappropriate web sites and by barring inappropriate items, terms and searches in both the Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

The school’s rules for safe Internet use accompany this letter. Please read and discuss these with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Principal.
St. Eugene’s Primary School’s acceptable use of the internet, emails and computers.

At St. Eugene’s Primary School we understand the importance and benefits of using computers to help with children’s learning and personal development. However, we also recognise that safeguards need to be in place to ensure children are kept safe. Please could parents/carers read and discuss this agreement with their child and then sign and return to their class teacher

➢ I will only use ICT in school 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 whom my teacher has approved.
➢ I will only log on using my own username and password which is confidential and not tell other people.
➢ I will only open/delete my own files.
➢ I will make sure that all ICT contact with others is responsible, polite and sensible.
➢ I will not send anyone material that could be considered threatening, offensive or illegal.
➢ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
➢ If I accidentally find anything nasty, accidently I will tell my teacher immediately.
➢ I will not give out my own details such as my name, phone number or home address.
    or arrange to meet anyone
➢ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
➢ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
➢ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.

➢ If I break these rules I know I may be stopped from using the internet and/or computers.

Parent and child’s signatures:

We have discussed this policy and…………………………………………………………………….(child’s name)

agrees to support the safe use of ICT at St. Eugene’s Primary School

Parent/ Carer’s Signature………………………………………………………………………………………..

Child’s Signature……………………………………………………………../………………….………………..Date…………………………...

Additional Advice for Parents with Internet Access at home

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 school 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 unsuitable 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 and teachers is available from the following sources:

www.saferinternet.org.uk/advice-centre/young-people/resources-3-11s
www.thinkuknow.co.uk Thinkuknow - a mock cyber-cafe which uses online role-play to help children from 5 to 16+ explore a range of issues.
www.kidsmart.org.uk/ Explains the SMART rules for safe internet use and lots more besides.
www.parents.vodafone.com Vodafone’s site is designed to help parents develop an understanding of their child’s internet use.
www.childline.org.uk/ Get child protection research, tools and resources for professionals, learn what works through impact and evidence and find services for children and families.

C2K provides e-safety support for all teachers in Northern Ireland. They have developed resources such as videos and DVD’s and editable PowerPoint presentations for teachers to use in lessons. They have also developed support documentation for schools to devise their own e-safety policies.

The PSNI also delivers CEOP’s Thinkuknow internet safety programme to primary and postprimary schools throughout NI as part of their Citizen and Safety Education (CASE) programme.

NSPCC has staff trained as CEOP ambassadors and also deliver the CEOP Thinkuknow introduction and Ambassador training to other organisations
NSPCC delivers the Childline Schools Service in NI primary schools which looks at online safety and cyber bullying
NIABF (Northern Ireland Anti-Bullying Forum) and Beat the Cyber Bully, both of which have undertaken substantive work specifically in the area of cyberbullying.

| Date of latest update: |  
| --- | --- |
| The Policy was agreed by governors on: |  
| The Policy is available for staff at: |  
| And for parents at: |  
| The designated Child Protection Teacher/Officer is |  
| The E-safety Coordinator is: |  
| Has E-safety training been provided for both pupils and staff? |  
| Do all staff sign an ICT Code of Conduct on appointment? |  
| Do children sign an agreement about responsible IT use? Are parents sent a copy of that? |  
| Have school E safety rules been set for pupils? |  

Staying Safe Online

1) Don’t post any personal information online – like your address, email address or mobile number.

2) Think carefully before posting pictures or videos of yourself. Once you have put a picture of yourself online most people can see it and may be able to download it, it’s not just yours anymore.

3) Keep your privacy settings as high as possible

4) Never give out your passwords

5) Don’t befriend people you don’t know

6) Don’t meet up with people you’ve met online. Speak to your parent or carer about people suggesting you do

7) Remember that not everyone online is who they say they are

8) Think carefully about what you say before you post something online

9) Respect other people’s views, even if you don’t agree with someone else’s views doesn’t mean you need to be rude

Are these rules displayed in all rooms with computers?

Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access

Has the school filtering policy been approved by the SMT?

Is personal data collected, stored and used according to the principles of the Data Protection Act 2018?
10) If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately.