Safeguarding in a Digital World Policy

(E- Safety & Internet Acceptable Use)

Reviewed April 2016 Mr Colhoun Staff Copy

As a Rights Respecting School, our pathway to a successful future is grounded in the United Nations Convention on the Rights of the Child (UNCRC).

ARTICLE 3: The best interests of the child must be a top priority in all things that affect children.

ARTICLE 16: Every child has the right to privacy. The law should protect the child's private, family and home life.

St. Paul's Primary School

Use of the internet, mobile phones, I pads and games

Internet – refer to school policy for internet use

Mobile phones

These phones have the potential to be used inappropriately e.g. cyber bullying, sexting, indecent photographs etc.
In St. Paul's our policy attempts to address use of mobile phones and safeguard our pupils.

- Restrictions on use
    - Mobiles must be given to the class teacher at the beginning of the school day (kept in teacher's drawer)
    - Returned to pupil at the end of the school day
    - Sanctions in place (parent must come to school to collect mobile phone)

- Use of mobile phones outside of school hours
    - Teachers' role – educate pupils in correct use of mobiles and consequences of their misuse (in particular during Anti Bullying Week)
    - Educate parents in monitoring their child's use of mobiles

- Close liaision with external agencies e.g. PSNI, NIABF etc.

Games

Awareness raising information given to parents during initial parent/ teacher meeting.

Close monitoring of games brought in from home.

Acceptable Use Policy for Internet Use

ICT is integrated in to the primary school curriculum and is used to support all subject areas. The Internet provides a valuable source of information and many sites are targeted to supplement the programmes of study in the Northern Ireland Curriculum. Pupils will be given opportunities to use the Internet as part of their learning.

Each classroom is now resourced with new computers, access to the school network and the Internet. Usually, the resources used by the pupils in school are carefully chosen by the teacher and determined by the curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these, to sites unfamiliar to the teacher.

The school believes that the benefits to pupils from access to the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information sources, is one the school shares with parents and guardians.

In St Paul's Primary, we feel that the best recipe for success lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.
Parents will be sent an explanatory letter and the rules, which form our Internet Access Agreement.

Pupils are responsible for good behaviour on the Internet just as they are in the classroom or a school corridor. General school rules apply.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards and will honour the agreements they have signed.

Computer storage areas, files and communications may be reviewed by teachers to insure pupils are using the system responsibly. Pupils should not expect that files stored on servers or discs would always be private.

Curriculum Use

Staff are encouraged to use Internet resources in their teaching and learning activities, to conduct research and for contact with others in the Educational world.

The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons. Use of the Internet is also seen as a means to improve Literacy skills, particularly being able to read and appraise critically and then communicate what is important to others.

Initially, the pupils may be restricted to sites, which have been reviewed and selected for content. They may be given tasks to perform using a specific group of websites which they may be able to access from a common favourite's folder. As pupils gain experience, they will be taught how to search using techniques to locate specific information for themselves and comparisons will be made between the various sources of information available to them. (CD ROM, books, WWW)

We hope that pupils will learn to decide when it is appropriate to use the Internet, as opposed to other sources of information, in terms of time taken: the amount of information found and the usefulness and reliability of information located.

At times information such as text, photos etc may be downloaded from the Internet for use in Pupils' presentations. Tasks will be set to encourage pupils to view web sites and information with a critical eye.

Guidelines for Internet Use

Staff and Pupils

a) When using the Internet, all users must comply with all copyright, libel, fraud, and discrimination and obscenity laws. 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.

b) Pupils are responsible for good behaviour on the school networks. The use of information and communication technologies is a required aspect of the statutory NIC.

c) Staff will ensure that pupils know and understand that no Internet user is permitted to:

- Send, copy or display offensive messages or pictures.(cyber bullying see anti bullying policy)
- use obscene language
- harass, attack or insult others
- damage computers, computer systems or computer networks
- violate copyright laws
- use another user's password
- trespass in another user's folders, work or files
- leave a computer unattended while user is logged on
- intentionally waste limited resources
- subscribe to any services or order any goods or services, unless specifically assigned by the teacher
- publish, share or distribute any personal information about a user
- enter competitions without first getting permission
- In the event of unsuitable material being displayed on the Internet pupils should immediately inform the class teacher.
- Inform parents of the potential risks associated with internet use in the home (initial parent meeting)

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet use.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

NB Please ensure that you have checked the updated list re: photographs

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
The school's e-Safety policy will operate in conjunction with other policies including those for UICT, Student Behaviour, Curriculum and Data Protection.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- ✓ Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

- ✓ Sound implementation of e-Safety policy in both administration and curriculum, including secure school network design and use.

- ✓ Safe and secure broadband from the C2K Network including the effective management of Websense filtering.

- ✓ National Education Network standards and specifications.

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- ✓ Our E-Safety Policy has been written by the school, building on a recent e-Safety course and government guidance. It has been agreed by senior management and approved by governors and teachers.

- ✓ The E-Safety Coordinator is Mrs Corrigan who is also the Child Protection Coordinator and a member of the Senior Leadership Team.

- ✓ The E-Safety Governor is Mrs Corrigan who is also the safe guarding governor.

- ✓ The E-Safety Policy and its implementation will be reviewed annually.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within St. Paul's Primary School.

Governors:

The role of the e-safety governor will include:

- ✓ Regular meetings with the e-safety co-ordinator
- ✓ Regular monitoring of e-safety incident logs
- ✓ Regular monitoring of filtering
- ✓ Reporting back at Governor meetings

Head teacher:

- ✓ The head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator
- ✓ The head teacher and at least another member of the SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- ✓ The head teacher is responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues
- ✓ The head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role

E-Safety Co-ordinator:

The role of the E-Safety Co-ordinator will include:

- ✓ Leading the e-safety committee
- ✓ Takes day to day responsibility for e-safety issues as well as reviewing the school e-safety policies
- ✓ Ensures all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- ✓ Provides training and advice for staff
- ✓ Liaises with the Local Authorities
- ✓ Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- ✓ Meets regularly with the E-Safety Governor
- ✓ Reports regularly to the SLT

ICT Co-ordinator:

The role of the technical staff will include:

- ✓ Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- ✓ Ensuring that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- ✓ Ensuring that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- ✓ Making sure they have an up to date awareness of e-safety matters and of the current e-safety policy and practices
- ✓ Ensuring that they have read, understood and signed the Staff Acceptable Use Policy
- ✓ Ensuring that they report any suspected misuse or problem to the Head teacher/E-safety Co-ordinator for investigation / action / sanction

Teaching and Support Staff:

The role of the teaching and support staff will include:

- ✓ having an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- ✓ Ensuring they have read, understood and signed the Staff Acceptable Use Policy
- ✓ Reporting any suspected misuse or problem to the Head teacher / E-Safety Coordinator for investigation / action / sanction
- ✓ All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- ✓ E-safety issues are embedded in all aspects of the curriculum and other activities
- ✓ Students / pupils understand and follow the e-safety and acceptable use policies
- ✓ Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ✓ That they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- ✓ in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils:

- ✓ Are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- ✓ Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ✓ Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- ✓ Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Teaching and learning

Why is Internet use important?

- ✓ Internet use is part of the statutory curriculum and is a necessary tool for learning.
- ✓ The Internet is a part of everyday life for education, business and social interaction.
- ✓ The school has a duty to provide students with quality Internet access as part of their learning experience.
- ✓ Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- ✓ The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- ✓ Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- ✓ • access to worldwide educational resources including museums and art galleries;
- ✓ • inclusion in the National Education Network which connects all UK schools;
- ✓ • educational and cultural exchanges between pupils worldwide;
- ✓ • vocational, social and leisure use in libraries, clubs and at home;
- ✓ • access to experts in many fields for pupils and staff;
- ✓ • professional development for staff through access to national developments, educational materials and effective curriculum practice;
- ✓ • collaboration across networks of schools, support services and professional associations;
- ✓ • improved access to technical support including remote management of networks and automatic system updates;
- ✓ • exchange of curriculum and administration data with KCC and DfE;
- ✓ • access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- ✓ The school's Internet access will be designed to enhance and extend education.
- ✓ Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- ✓ The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- ✓ Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- ✓ Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- ✓ 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 to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

- ✓ Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- ✓ Pupils will use age-appropriate tools to research Internet content.
- ✓ The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained?

- ✓ The security of the school information systems and users will be reviewed regularly.
- ✓ Virus protection will be updated regularly via C2K.
- ✓ Personal data sent over the Internet or taken off site will be encrypted.
- ✓ Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- ✓ Unapproved software will not be allowed in work areas or attached to email.
- ✓ Files held on the school's network will be regularly checked.
- ✓ The ICT coordinator/network manager will review system capacity regularly.
- ✓ The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

- ✓ Pupils may only use approved email accounts for school purposes.
- ✓ Pupils must immediately tell a designated member of staff if they receive offensive email.
- ✓ Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- ✓ Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- ✓ Access in school to external personal email accounts may be blocked.
- ✓ Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- ✓ Schools will have a dedicated email i.e. (Mrs Corrigan) for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

How will published content be managed?

- ✓ The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- ✓ Email addresses will be published carefully online, to avoid being harvested for spam
- ✓ The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- ✓ The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

- ✓ Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- ✓ Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- ✓ Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- ✓ Pupils work can only be published with their permission or the parents.
- ✓ Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- ✓ The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

How will social networking, social media and personal publishing be managed?

- ✓ The school will block all access to social media and social networking sites.
- ✓ Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- ✓ Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

- ✓ Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- ✓ All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- ✓ Concerns regarding students' use of social networking, social media and personal publishing sites (out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- ✓ Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How will filtering be managed?

- ✓ The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- ✓ The school will work with C2K to ensure that filtering policy is continually reviewed.
- ✓ The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- ✓ If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- ✓ The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- ✓ Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- ✓ The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- ✓ Any material that the school believes is illegal will be reported to appropriate agencies.
- ✓ The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

How are emerging technologies managed?

- ✓ Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- ✓ Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

How should personal data be protected?

- ✓ Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

How will Internet access be authorised?

- ✓ The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- ✓ All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- ✓ Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- ✓ All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- ✓ Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- ✓ When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- ✓ At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- ✓ At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will risks be assessed?

- ✓ The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor C2K can accept liability for the material accessed, or any consequences resulting from Internet use.
- ✓ The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- ✓ The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to PSNI.
- ✓ Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

- ✓ All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, Cyberbullying, illegal content etc.).
- ✓ The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- ✓ The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- ✓ The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- ✓ The school will inform parents/carers of any incidents of concerns as and when required.
- ✓ After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- ✓ Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the PSNI.
- ✓ If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- ✓ If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to the PSNI.

How will e–Safety complaints be handled?

- ✓ Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- ✓ Any complaint about staff misuse will be referred to the head teacher.
- ✓ All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- ✓ Pupils and parents will be informed of the complaints procedure.
- ✓ Parents and pupils will need to work in partnership with the school to resolve issues.
- ✓ All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- ✓ Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- ✓ Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- ✓ All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community?

- ✓ The school will liaise with local organisations to establish a common approach to e–Safety.
- ✓ The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- ✓ The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- ✓ The school will provide a (Guest Account) for any guest who needs to access the school computer system or internet on site.

How will Cyberbullying be managed?

- ✓ Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- ✓ There are clear procedures in place to support anyone in the school community affected by Cyberbullying.
- ✓ All incidents of Cyberbullying reported to the school will be recorded.
- ✓ There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- ✓ Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- ✓ The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- ✓ Pupils, staff and parents/carers will be required to work with the school to support the approach to Cyberbullying and the school's e-Safety ethos.
- ✓ Sanctions for those involved in Cyberbullying may include:

    - ✓ The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - ✓ Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - ✓ Parent/carers of pupils will be informed.
    - ✓ The Police will be contacted if a criminal offence is suspected.

How will mobile phones and personal devices be managed?

- ✓ The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use of Mobile Phone Policies.
- ✓ The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- ✓ School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- ✓ Mobile phones and personal devices will not be used during lessons or formal school time by staff.
- ✓ Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- ✓ Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- ✓ Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.

Pupils Use of Personal Devices

- ✓ Pupil's mobile phones will be kept in the school office.
- ✓ If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- ✓ If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- ✓ Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- ✓ Staffs are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- ✓ Staff will be issued with a school phone where contact with pupils or parents/carers are required.
- ✓ Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- ✓ If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- ✓ Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- ✓ If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

How will the policy be introduced to pupils?

- ✓ All users will be informed that network and Internet use will be monitored.
- ✓ An e-Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- ✓ Pupil instruction regarding responsible and safe use will precede Internet access.
- ✓ An e-Safety module will be included in PDMU or ICT programmes covering both safe school and home use.
- ✓ e-Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- ✓ e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- ✓ Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- ✓ Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- ✓ The e-Safety Policy will be formally provided to and discussed with all members of staff.
- ✓ To protect all staff and pupils, the school will implement Acceptable Use Policies.
- ✓ Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- ✓ Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- ✓ Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- ✓ The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.

- ✓ All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

- ✓ Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- ✓ A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e-Safety at other attended events e.g. parent evenings and sports days.
- ✓ Parents will be requested to sign an e-Safety/Internet agreement as part of the Home School Agreement.
- ✓ Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- ✓ Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.
- ✓ Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- ✓ Interested parents will be referred to organisations listed in the "e-Safety Contacts and References section".

Helpful Links

e-Safety Contacts and References
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://www.nidirect.gov.uk/click-clever-click-safe
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
EIS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
PSNI
Kidsmart: www.kidsmart.org.uk
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Department of Education
http://www.deni.gov.uk/index/pupils-and-parents/pupils.htm
www.getsafeonline.org
http://safeguardingni.org/

The following advice has been supplied by the PSNI and endorsed by the Safeguarding Board for Northern Ireland (SBNI).

This information will also be available on the C2K exchange.

Detailed advice and guidance on eSafety is available to teachers within an eSafety Zone, also available via the C2k exchange. C2k will be offering further training and support in the entire area of eSafety to all schools during the coming year.

Letter sent from the Department of Education on 15.6.2015

Pupil Support Team

Department of
Education
www.deni.gov.uk
AN ROINN
Oideachais
MÄNNYSTRIE O
Lear

Rathgael House
43 Balloo Road
Rathgill
Bangor
BT19 7PR

12 June 2015

To:

Principals and Boards of Governors of all grant-aided schools
Education Authority
Council for Catholic Maintained Schools
Northern Ireland Council for Integrated Education
Comhairle na Gaelscolaíochta
Governing Bodies Association
Proprietors of Independent Schools
CCEA
YCNI

Dear Colleagues

Inappropriate use of the internet and mobile technologies, such as trolling, sexting, Cyberbullying or sexual exploitation, can, as we are all aware, have a devastating impact on the lives of our children and young people.

As we approach the summer holidays it may therefore be timely to think about what information might be passed on to children and young people and their parents to address any questions or concerns that they might have. The following advice has been supplied by the PSNI and endorsed by the Safeguarding Board for Northern Ireland (SBNI) and may help Head Teachers draft letters to parents but also give teachers and those in the Youth Service, some simple advice. This information will also be available on the C2K exchange.

General advice to everyone:

We all deserve to be able to use the internet to learn, explore and connect with each other. But all of us need to be aware of the risks involved in doing so, especially on social media. Our advice is:

- Don't share personal information or images with people you don't know.

- Don't accept friend requests with someone you don't know – not everyone online may be who they say they are.

- Set privacy settings on all devices so that only people you know can view your account.

- Don't post anything online that you are not happy to be shared, particularly nude or nearly nude images or videos. It may seem like a bit of fun with friends at the time but there is always a chance those images could be shared or get into the wrong hands and could lead to harmful situations such as stalking, abuse or blackmail.

- If someone has made you feel uncomfortable or you have had disturbing interaction online, tell police or a trusted adult. You can ring the police on 101 or for help and advice ring Childline on 0800 1111 or Lifeline on 0808 808 8000.

- The internet can be a great place but it is important to remember there are people out there who may wish to abuse, exploit, intimidate or bully you online – if this happens to you, tell someone immediately.

- Remember that if things do go wrong online, there are people who can help.

- If you receive any inappropriate images or links, it is important that you do not forward it to anyone else. Contact police or tell a trusted adult immediately. By doing this you could help prevent further such incidents. You will not get into trouble.

General advice to parents:

- The most important thing is to have conversations with your children - talk to them about the benefits and dangers of the internet so that you can empower them to use the internet safely.
- Cultivate an interest in their online activities - their favourite websites, online games and interests and keep an eye on what they are doing online.
- Don't be afraid to ask your children who they are talking to online and what they are talking about and remind them how important it is to tell a trusted adult if something happens online that makes them feel uncomfortable or worried because there are people who can help.
- Become a 'net-savvy' parent - the best safeguard against online dangers is being informed. Jump in and learn the basics of the Internet - read articles, take a class, and talk to other parents. You don't have to be an expert to have a handle on your child's online world.
- Go to www.getsafeonline.org for lots of useful advice and information on how to stay safe online. Safeguardingni.org will also provide information for parents and carers on e-safety.
- Links to other sites that can provide information and advice to young people and parents are available from the DE website at: http://www.deni.gov.uk/index/pupils-and-parents/pupils.htm

The Department will continue to share information and advice with schools and other educational establishments as it becomes available.

Yours sincerely

ANGELA KANE
Head of Pupil Support Team

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to ICT Coordinator	Refer to Principal	Refer to Police	Refer toC2k for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X	
Unauthorised use of non-educational sites during lessons	X	X					X	X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X				X	X	
Unauthorised use of social media / messaging apps / personal email	X	X	X				X	X	
Unauthorised downloading or uploading of files	X	X	X				X	X	
Allowing others to access school / academy network by sharing username and passwords	X	X	X						
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X	X						
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X	X		X				
Corrupting or destroying the data of other users	X	X	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X				
Continued infringements of the above, following previous warnings or sanctions	X	X	X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X						
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X	X	X				
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X				
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X						

Staff

Actions / Sanctions

Incidents:	Refer to ICT Coordinator	Refer to Principal	Refer to Local Authority / HR	Refer to Police	Refer to C2k for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X	X						
Unauthorised downloading or uploading of files	X	X			X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X						
Careless use of personal data eg holding or transferring data in an insecure manner	X	X						
Deliberate actions to breach data protection or network security rules	X	X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X						
Actions which could compromise the staff member's professional standing	X	X						
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X						
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X						
Deliberately accessing or trying to access offensive or pornographic material	X	X						
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X						

Violations of this Expected Use Policy Violations of this policy in St. Paul's Primary may have disciplinary repercussions, including:

- Suspension of computer privileges
- Notification to parents in most cases
- Detention
- Suspension from school and/or school-related activities
- Expulsion