**St Mary’s Primary School Ballygawley**



**E-Safety Policy**

**Date:** June 2023

**Review Date:** June 2026

Signature of Chair of BOG: Austin Walsh

Signature of School Principal: Cara Donnelly

**Introduction**

Boards of Governors have a duty to safeguard and promote the welfare of pupils (Article 17 of the Education and Libraries (Northern Ireland)

Order 2003). It is also the duty of the Board of Governors to determine the measures to be taken at a school to protect pupils from abuse (Article 18 of the Education and Libraries (Northern Ireland) Order 2003 refers).

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: these will serve to reassure parents and guardians.

This E-safety policy contains policies in relation to use of the internet, use of mobile phones and use of digital/photographic images of children. It is largely based on DENI Circular 2007/1 *“Acceptable Use of the Internet and Digital Technologies in Schools”* , DENI Circular 2011/22 *“Internet Safety”* and DENI Circular 2013/25 *“eSafety Guidance”.*

The policy relates to other policies including Using ICT, Internet Code of Conduct, Anti-Bullying, Child Protection, Positive Behaviour and Health and Safety.

**Internet Safety Policy**

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 for education, business and social interaction. Our school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

The DENI circular 2007/01 states that:

*“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.”*

This document sets out the policy and practices for the safe and effective use of the Internet in St Mary’s P.S. The policy has been drawn up by the staff of the school, under the guidance of Mrs Donnelly (Principal) and Mr Donaghy (ICT coordinator). It has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested.

The policy and its implementation will be reviewed annually.

**Teaching and Learning**

The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school’s management information and business administration systems.

Access to the internet is a necessary tool for staff and students. It helps to prepare students for the future and is used across a range of subjects

**3. C2K**

Classroom 2000 (C2k) is the project responsible for the provision of 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. Filters access to websites.
* Providing appropriate curriculum software.

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. At present we do not use other service providers.

**Email**

* Pupils may only use C2k e-mail accounts on the school system.
* Pupils must immediately tell a teacher if they receive an offensive e-mail or other form of message.
* Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
* The forwarding of chain mail is not permitted.

• Children are not always given individual e-mail addresses. In some instances, children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

**Social networking**

* The school C2k system will block access to social networking sites.

• Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.

• Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

• Our pupils are asked to report any incidents of bullying to the school.

• School staff will not add children as ‘friends’ if they use these sites.

**Mobile technologies**

* The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.

• Staff should not store pupils’ personal data and photographs on memory sticks. • Pupils are not allowed to use personal mobile devices/phones (in school) during class.

• Staff should not use personal mobile phones during designated teaching sessions

**Managing Video-Conferencing**

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

**Publishing Pupils’ Images and Work**

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

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

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

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

• Pupil’s work can only be published by outside agencies with the permission of the pupil and parents.

**Policy Decisions: Authorising Internet access**

• Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school’s e-Safety rules. These eSafety rules will also be displayed clearly in all rooms. • Access to the Internet will be supervised.

• All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school’s e-Safety rules and within the constraints detailed in the school’s e-Safety policy.

• All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

**Password Security**

• Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils. • All pupils are provided with an individual login username and password.

• Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.

• Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

**Handling e-Safety Complaints**

• Complaints of Internet misuse will be dealt with by the Principal

• Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the e-Safety incident logbook. • Any complaint about staff misuse must be referred to the Principal.

• Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

• Pupils and parents will be informed of the complaints’ procedure.

**Cyberbullying**

Instances of cyber bullying of pupils or staff will be regarded as a very serious offence and dealt with according to the school’s Positive Behaviour Policy and Child Protection and Safeguarding Policy. However, it is the responsibility of parents to monitor and manage their children’s personal use of technology and the internet at home when not using C2k or school aligned services.

**Communicating the Policy: Introducing the e-Safety Policy to pupils**

* E-Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year.
* Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week/ Internet Safety Day.
* Pupils will be informed that network and Internet use will be monitored.

**Staff and the E-Safety Policy:**

• All staff will be given the School e-Safety Policy and its importance explained. • Any information downloaded must be respectful of copyright, property rights and privacy.

• Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.

• A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school

**Roles and Responsibilities**

As e-Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school. The ICT / E-Safety Co-ordinator liaises regularly with the Safeguarding Team and meets annually with the Designated Governor for Child Protection. Mrs Patricia Hagan is Designated teacher for Child Protection, Mrs Cara Donnelly and Mr Stephen Donaghy are deputy designated teachers for Child Protection. All governors are regularly updated on the issues at our school in relation to local and national guidelines and advice. Mrs Pauline Mc Ginley has been designated as governor responsible for Child Protection.

**Health and Safety**

In St Mary’s Primary School we have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both, which has been designed in accordance with health and safety guidelines. 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, interactive whiteboard and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are 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.  Further information on WiFi equipment is available at: [the Health Protection Agency website](http://www.hpa.org.uk/web/HPAweb&HPAwebStandard/HPAweb_C/1241418705217).

**School Website**

The school website is used to celebrate pupils' work, promote the school and provide information. Editorial guidance will ensure that the Website reflects the school's ethos that information is accurate and well-presented and that personal security is not compromised. An editorial team ensure common values and quality control. As the school's Website 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 Website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
* Website photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
* Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
* The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
* The Website 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.

**Implementing E-safety for Pupils**

The education of pupils in e-safety is essential. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience. The aim is to develop children’s e-safety skills for when they are in school and outside of school. E-Safety education should be provided in the following ways:

* Planned e-safety activities should be incorporated into PDMU and other lessons, where appropriate. (For e.g. within literacy – creating a poster/news sheet, reading non-fiction texts, giving a presentation etc.)
* Key e-safety messages should be reinforced as part of a planned programme of assemblies and whole school activities e.g. participation in an Internet Safety Week or Safer Internet Day. Visit from PSNI.
* Children should research e-safety and become familiar with key websites such as www.thinkuknow.co.uk and use the information to create resources to raise parental/peer awareness of safety messages. The children can create posters, presentations, short films or podcasts on e-safety and display these within school and at home. (e-safety can be the focus for many CCEA tasks)
* Encourage children to discuss e-safety with parents/carers – look at a website together, discuss an esafety poster etc. This can form part of a homework task.
* SMART safety rules should be displayed in classrooms and should be discussed and referred to regularly.
* Children should participate in devising and agreeing to an AUP and encouraged to adopt a safe and responsible use of ICT, the internet and mobile devices both within and outside school.
* The School Council may focus on e-safety issues.

**Parents / Carers**

Many parents and carers have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children’s online experiences. Parents often either underestimate, or do not realise, how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school should therefore seek to provide information and awareness to parents and carers in the following ways:

• Put links to e-safety information and resources on the school website.

• Include e-safety tips on the school website – embed the \*“Childnet” banner.

• Use opportunities when parents/carers are in school - provide leaflets at parent interviews, curriculum evenings, open days, parent assemblies, etc.

• Have children carry out e-safety research with parents and discuss web materials, posters etc.

• Put e-safety tips in the school newsletter.

• Share the e-safety policy – make it available on the school website and in the school.

• Display e-safety information where parents/carers gather in the school at collection points. [www.childnet-int.org/publications/resources.asp](http://www.childnet-int.org/publications/resources.asp).

**Staff**

Staff should be involved in formal discussions about e-safety and have opportunities to participate in e-safety training. An audit of the e-safety training needs of all staff may be carried out.

• The ICT Coordinator will keep up to date on e-safety through attendance at INSET and by reviewing guidance documents released by agencies such as CEOP/DE/EA and others. The ICT Co-ordinator should seek planned opportunities to disseminate this information to all staff.

• The E-Safety Policy should be discussed and reviewed by staff during staff meetings or on INSET days.

• Staff should be familiar with e-safety websites such as Childnet’s “Know it all for Teachers” or CEOP’s “ThinkuKnow”. (see below)

• Implementing E-safety may be part of agreed PRSD targets for the whole school.

• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Policies.

• Teachers should share good practice in implementing e-safety and ensure e-safety activities are included in planning for PDMU and other curriculum areas.

**Governors**

Governors should be encouraged to take part in e-safety training or awareness sessions. This has particular importance for those who are members of any sub- group involved in health and safety /child protection.

This may include:

* Attendance at e-safety events.
* Participation in school training/information sessions for staff or parents.
* The ICT Co-ordinator meeting with the Governors to update them on e-safety issues and procedures within the school.
* Consultation with regard to the e-safety Policy.
* Accessing e-safety information which is available on the school website or in parent leaflets and newsletters.

**Monitoring and Review**

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator. It has been agreed by staff and approved by the Governing Body. This policy is the Governors’ responsibility and they will review its effectiveness bi-annually. They will do this during reviews conducted between the ICT Co-ordinator and the Designated Child Protection Team.

**Writing and Reviewing the E-Safety Policy**

This policy, supported by the school’s Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

Appendix 1

**ICT Code of Safe Practice**

**(Primary Pupils P1-P3)**

**eSafety Rules**

* I will only use the internet when an adult is with me.
* I only click on links and buttons online when I know what they do.
* I keep my password safe.
* I only send messages online which are polite and friendly.
* I know my teachers can see what I am doing online when I use school computers and iPads.
* I always tell a teacher or trusted adult if something online makes me feel upset, unhappy, or worried.
* I know that if I do not follow the rules, I may not be allowed to use school computers or iPads.
* I have read and talked about these rules with my parents/carers.

Appendix 1

**ICT Code of Safe Practice**

**(Primary Pupils P4-P7)**

**eSafety 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 when e-mailing.
* I will only open e-mail attachments from people I know, or who my teacher has approved.
* I will not tell other people my ICT passwords.
* I will only open/delete my own files.
* I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
* I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
* I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
* I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
* I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-Safety.

Appendix 2

**Parental Agreement/Consent Letter**

**(Primary Pupils)**

Dear Parent/ Carer

As part of St Mary’s P.S. 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 Mrs Donnelly.

**✂**

**Parent/ carer signature**

We have discussed this and ……………………………………..........(child name) agrees to follow the E-Safety rules and to support the safe use of ICT at St Mary’s Primary School.

Parent/ Carer Signature ……………………….…………………………. Date ………………………

Appendix 3

**ICT Code of Safe Practice** **for Staff**

**eSafety Rules**

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

* 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 pupils and 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 Board of Governors. Personal or sensitive data taken off site must be encrypted.
* I will not install any hardware or software without permission of the Principal.
* I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
* Images of pupils and/ or staff will only be taken, stored and used for professional purposes online with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
* 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 Line Manager or 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.

**User Signature**

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

Signature …….………………….………………. Date ……………………

Full Name …………………………………….... (printed) Job Title . . . . . . . . . . . . . . ...

Appendix 4

**Sample Posters**

**Key Stage 1**

|  |  |  |
| --- | --- | --- |
| Think then Click | | |
| These rules help us to stay safe on the Internet | | |
|  | We only use the internet when an adult is with us |  |
|  | We can click on the buttons or links when we know what they do. |  |
|  | We can search the Internet with an adult. |  |
|  | We always ask if we get lost on the Internet. |  |
|  | We can send and open emails together. |  |
|  | We can write polite and friendly emails to people that we know.  B. Stoneham & J. Barrett |  |

Key Stage 2

|  |
| --- |
| **Think then Click** |
| e-Safety Rules for Key Stage 2 |

**Principles for Internet Use ----- Children’s Version**

Be **SMART** On Line

|  |  |
| --- | --- |
| **S** | **Secret**  Never give your address, telephone number, username or password when on-line. |
| **M** | **Meeting** someone or group you have contacted on-line is not allowed without the permission and supervision of your parent or teacher. |
| **A** | **Acceptin**g e-mails, opening sites or files requires the permission of your teacher, appointed adult or parent. |
| **R** | **Remembe**r no offensive language, text or pictures are to be displayed, sent, copied or received. |
| **T** | **Tell** your parent, teacher or trusted adult if someone or something makes you uncomfortable. |

**Smile and Stay Safe Poster**

**E- Safety guidelines to be displayed throughout the school**

** and stay safe**

**S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

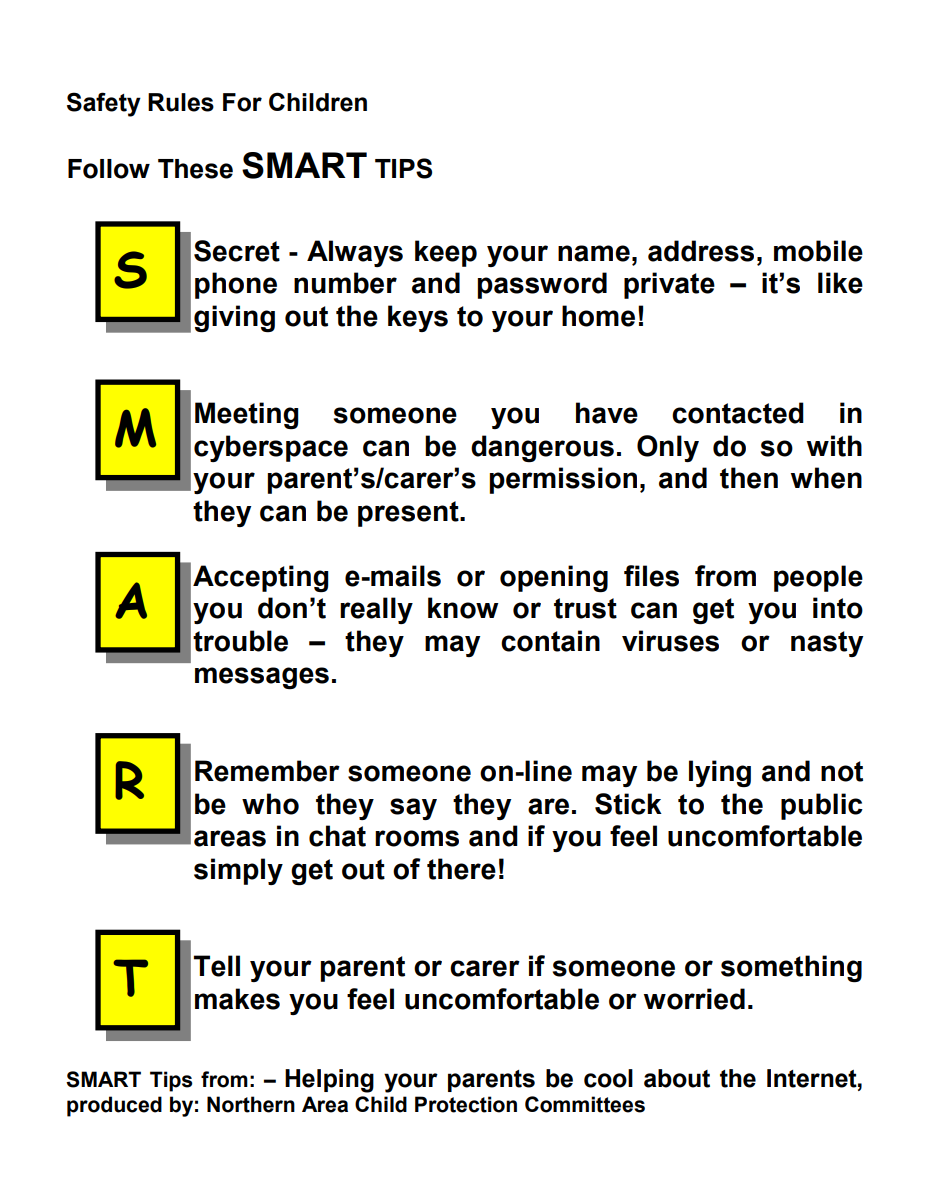
**M**eeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

**I**nformation online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

**L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

**E**mails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.



****

**Appendix 5: Social Media Policy**

**Rationale**

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

**Scope of Policy**

This policy covers all staff, pupils, governors, volunteers, placement students. They will be collectively referred to as Staff in this policy. Parents or community users who have access to our equipment are also required to comply with this policy. This policy deals with the use of all forms of social media, including Facebook, YouTube and Twitter, and all other social networking sites, internet postings and blogs. It applies to use of social media for school purposes as well as personal use that may affect the school in any way.

**School Use of Social Media**

Staff setting up a school account should:

• Notify the Internet Safety Co-ordinator, Mr Donaghy and forward details (intended audience, platform, staff in charge and shadow member of staff). This should be recorded by Mr Donaghy and Mrs Donnelly should be informed.

• Staff should regularly monitor, update and manage the content posted.

• Staff should ensure all pupils understand and agree with the guidelines.

• Staff should report any online incidents to Mr Donaghy

• Ensure communication is professional

**Personal/ Private Use of Social Media**

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

**Guidelines for Responsible Use**

Staff must not post disparaging or defamatory statements about:

1. The school

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

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

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

5. Other affiliates or stakeholders

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

Ensure profile and any content posted are consistent with the professional image you wish to present. If you disclose your affiliation with the school on your profile or in any social media postings, you must state that your views do not represent those of your employer. Staff should not accept as a ‘friend’ any pupil currently enrolled at the school or any past pupil under the age of 18. The exception to this is if the pupil is a family member. Staff should exercise their own discretion in this case. Staff should ensure that their settings on social media are set in such a way that protects their privacy. This applies to all postings, photographs and images.

**Social Media: Prohibited Use**

* Avoid communications that could damage the school’s reputation, even indirectly.
* Do not use social media to defame or disparage the school, management, staff, or any third party
* Do not use social media to harass, bully or unlawfully discriminate against staff or third parties
* Do not use social media to make false or misleading statements
* Do not use social media to impersonate colleagues or third parties
* Do not express opinions on the school’s behalf, unless expressly authorised to do so
* Do not include the school logo in any posting or in your profile
* Do not post comments about pupil performance. Any misuse of social media should be reported to Mr Donaghy (Internet Safety Coordinator) or Mrs Donnelly.

**Appendix 5**

**Additional Advice for Parents with Internet Access at home**

1. Any device 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 unsavoury materials. Further information is available from Parents’ Information Network (address below);

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

7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school, they should immediately inform the school.

Further advice for parents is available from the following sources:

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

<http://www.parents.vodafone.com>Vodafone’s site is designed to help parents and carers develop an un