**St. Joseph’s P.S.**

**Antrim**

**E-SAFETY POLICY**

**Including:**

* **Acceptable Use of the Internet & Digital Technology**
* **Internet Safety Policy**
* **Use of Photography and Videos**
* **Social Media Policy – incl. Twitter and Facebook**



Policy Review Date: November 2022

Date approved by Governors: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Chair of Governors: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Review Date: November 2024

**Acceptable Use of the Internet & Digital** **Technology Policy**

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and digital Technologies in Schools.

**Introduction**

In St. Joseph’s Primary School we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform learning and teaching when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This 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 in a safe, responsible manner.

The above circular 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 safe and effective use of the internet in

St. Joseph’s Primary School. The policy has been drawn up by the ICT Coordinator and Principal. It has been approved by governors and is available to all parents. The policy and its implementation will be reviewed bi-annually.

**Code of Safe Practice**

When using the internet, e-mail systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. The Code of Safe Practice for St. Joseph’s Primary School makes explicit to all users (staff and pupils) what is safe and acceptable and what is not.

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

The ICT Coordinator will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

**Code of Practice for Pupils**

Pupil access to the Internet is through a filtered service provided by C2K, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents on an annual basis before pupils access the Internet.

In addition, the following key measures have been adopted by St. Joseph’s to ensure our pupils do not access any inappropriate material:

* The school’s Code of Practice for use of the Internet and other digital technologies (E-Safety Agreement, see Appendix 1) is made explicit to all pupils.
* Pupils using the Internet will normally be working in highly-visible areas of the school.
* All online activity is for appropriate educational purposes and is supervised.
* 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 programmes. (Think U Know, saferinternetday.org, etc)

It should be accepted, however, that as rigorous as these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances. The school system is also monitored by the Securus system which alerts the Principal and Vice-Principal of any incidences of inappropriate search terms used in the system. The school has also adopted the Safer Schools app in the year 2021/2022. Any issues or concerns raised due to inappropriate searches or breaches of the filtering system will be dealt with by the Principal or Vice-Principal and recorded in the ‘Online Incident Register’ (see Appendix 2).

The use of mobile phones by pupils is not permitted on the school premises during school hours, unless in exceptional circumstances, where permission may be granted by the class teacher or Principal/Vice Principal. Mobile phones brought into the school building must be placed securely in the office for safe keeping. Due to the ever-changing nature of digital technology and the ability to record, pupils are not permitted to bring Smart watches to school.

**Sanctions**

Incidents of technology misuse which arise will be dealt with in accordance with the school’s discipline policy. Minor incidents will be dealt with by the Principal/Vice –Principal/ICT Coordinator and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with school child protection procedures.

**Code of Practice for Staff**

Staff adhere to the following Code of Safe Practice:

* Pupils accessing the Internet should be supervised by an adult at all times.
* All pupils are aware of the rules for the safe and effective use of the Internet. These are displayed in the ICT room and discussed with pupils.
* 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 C2K manager.
* Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
* Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
* Photographs of pupils should, where possible, be taken with a school iPad and images should be stored on a centralised area on the school network, accessible only to teaching staff.
* School systems may not be used for unauthorised commercial transactions.

**Internet Safety Awareness**

In St. Joseph’s we believe that, alongside having a written 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.

**What are the Dangers?**

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable.

**Internet Safety Awareness for pupils**

Rules for the Acceptable use of the Internet are discussed with all pupils and are displayed. In addition, Key Stage 2 pupils follow a structured programme of Internet Safety Awareness using a range of online resources. Eg. CEOP, Think You Know programmes. All children also participate in Internet Safety Day each year and revisit safety websites. Pupils and staff are involved in internet safety through our NAACE award mark for ICT which is reviewed every 3 years.

**Internet Safety Awareness for Staff**

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety and attends regular courses. This training is then disseminated to all teaching staff, classroom assistants and supervisory assistants on a regular basis.

Points for teachers to consider:

* Internet use should be planned, task orientated and educational within a regulated and managed environment.
* *Supervision is the key strategy*. Children should have a teacher or classroom assistant present when using the Internet. Computers should be positioned so that it is possible for adults to see materials on screen.
* Children should know why they are using the Internet. Teach children to use the Internet in response to a need. E.g. to answer a question which has arisen from work in class.
* Search engines require careful use and planning/supervision. Children can be bombarded with information and yet fail to find the material they need.
* Children do not need thousands of website addresses. A small appropriate choice is much more effective.
* Individual e-mail addresses may not be considered appropriate for younger children
* Teams (Primary 4-7) and Seesaw (primary 1-3) will be used as the mediums for setting and collecting online weekly homework tasks.
* Discuss with pupils the rules for responsible Internet use. It is not enough to protect children from materials, we must teach them to become Internet Wise.
* Children need to learn to recognise and avoid the risks.
* Children need to know what to do if they come across inappropriate material or if they are approached by a stranger.

**C2K Internet Filtering**

C2K filtering includes three internet security groups to which schools can add users to allow access to additional sites. Access to these groups is at the discretion of the Principal alongside the ICT Co-ordinator and requests from class teachers.

The three groups are:

**Internet Advanced**:  This group contains a number of sites that were previously accessible by all users in primary schools (eg. webmail, shopping, sex education and lifestyle sites).  As such, you may wish to consider adding all staff to this security group in order to facilitate a smooth transition.

**Internet Social Networking**:  This group contains Twitter, Facebook and LinkedIn.

**Internet Streaming Media**:  This group contains YouTube, Vimeo, BBC iPlayer and other mainstream video streaming sites

**Health & Safety**

St. Joseph’s have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the ICT suite, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and ICT equipment are being used.

**Policy Review**

Internet technology and school use of resources will develop and change with time. It is our responsibility to revise and up-date our Internet Safety Policy as appropriate and where necessary.

**Acceptable us of the internet policy amendments in line with new remote/blended or hybrid learning as a result of Covid-19**

As a result of the current Covid-19 pandemic, St.Joseph’s have been prepared to implement remote/blended or hybrid learning, including live streaming, as well as other forms of online communication to provide formal education and to stay in touch with our pupils and their parents or carers.

Following a thorough evaluation of the remote learning tools for use at whole school level and at key stage level, we have reviewed our acceptable use of the internet procedures to ensure safer practice in the event of a transition to remote or blended learning for both our pupils and staff.

Remote learning

* Remote/blended learning in St.Joseph’s will only take place using the online platforms of Seesaw (for communication in years 1-7 and for learning in years 1-3) and Microsoft Teams (for learning in years 4-7)
* Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
* Staff will use work provided equipment where possible (C2K managed school laptop or staff iPad)
* Where staff must use personal devices for remote learning, the expectations will remain clear in relation to safeguarding and data security when using personal devices e.g. using strong passwords, suitable levels of encryption, logging off or locking devices when not in use.
* Online contact with pupils and/or parents/carers will not take place outside of the operating times as defined by Mrs Treacy/ senior leadership team (9am-4.30pm)

Data protection and security

* Any personal data used by staff and captured by C2K when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy
* Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements

Session management

* Appropriate privacy and safety settings will be used to manage access and interactions through Seesaw and Microsoft Teams. This includes: disabling/limiting chat for pupils, staff not permitting learners to share screens, keeping meeting IDs private and discussion forum expectations being made explicit to pupils and continuously monitored by the class teacher/ other administrators.
* Access links to other learning platforms/programmes should not be made public or shared by participants.
* Pupils and/or parents/carers should not forward or share access links.
* If pupils/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
* Pupils are encouraged to attend lessons in a shared/communal space or room with an open door and appropriately supervised by a parent/carer or another appropriate adult.
* Alternative approaches and/or access will be provided to those who do not have access (iPad provided or work pack sent home).

Behaviour expectations

* Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
* All participants are expected to behave in line with existing St.Joseph’s behaviour policies and expectations.
* Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
* When sharing videos and/or live streaming, participants are required to:
* wear appropriate dress.
* ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
* Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Reporting concerns

* Participants are encouraged to report concerns during remote and/or live streamed sessions.
* If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to Mrs Treacy and/or the Vice Principal
* Any safeguarding concerns will be reported to our child protection officer, Mrs Treacy, in line with our child protection policy.

**Internet Safety Policy**

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circulars 2011/22, 2013/25 and 2016/27 on Online Safety. This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in St. Joseph’s Primary School. It also links to Article 17 from the UN Convention on the Rights of the Child which states:

*“You have the right to get information that is important to your well-being, from radio, newspaper, books, computers and other sources. Adults should make sure the information you are getting is not harmful, and help you find and understand the information you need.”*

St. Joseph’s Primary School Online Safety Policy reflects the importance we place on the safe use of information systems and electronic communications. It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. Online safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibility of using information technology.

**Online Safety:**

* is concerned with safeguarding children and young people in the digital world;
* emphasizes learning to understand and use technologies in a positive way;
* is less about restriction and focuses on educating children about the risks as well as the benefits so that users feel confident online;
* is concerned with supporting children and young people to develop safer online behaviours both in and out of school;
* prepares pupils to recognize unsafe situations and how to respond to risks appropriately.

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

The rapidly changing nature of the Internet and new technologies means that Online Safety is an ever growing and changing area of interest and concern. Our school policy reflects this by keeping abreast of the changes taking place. We as teachers have a duty of care to enable pupils to use on-line systems safely. This policy operates in conjunction with other school policies including Positive Behaviour, Child Protection/Safeguarding Children and Antibullying. Online Safety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the Northern Ireland curriculum and schools must ensure acquisition and development by pupils of these skills.

 Online Safety in St. Joseph’s 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 internet provision by C2K and C2K Wireless systems.

**Roles and Responsibilities:**

Online Safety is an important aspect of Child Protection/Safeguarding Children within the school therefore, the ICT Co-ordinator, Vice-Principal, 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 and Designated Teacher (DT) to keep abreast of current online safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. This team has the responsibility for leading and monitoring the implementation of online safety throughout the school.

The Online Safety Team have the responsibility to update staff and Governors with regard to Online Safety and all governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice.

**ICT Co-ordinator:**

Our ICT coordinator is the person responsible for the day-to-day issues relating to Online Safety.

* takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies/documents,
* ensures that all staff are aware of the procedures that need to be followed in the event of an incident,
* provides training and advice for staff,
* receives reports of Online Safety incidents and creates a log of incidents to inform future developments,
* receives appropriate training and support to fulfil his/her role effectively,
* passing on requests for blocking/unblocking to the C2K and/or Classnet helpdesks.

**The Board of Governors:**

* are responsible for the approval of this policy and for reviewing its effectiveness. The governors should receive regular information about Online Safety incidents and monitoring reports.

**The Principal:**

* is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety is delegated to the online safety co-ordinator;
* and the Vice-Principal 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. Refer to staff disciplinary procedures, and/or Child Protection/Safeguarding Children Policy.

**Teaching and Support Staff must:**

* have an up-to-date awareness of online safety matters and of the current school online safety policy and practices;
* embed online safety issues into the curriculum and other school activities as appropriate;
* have read, understood and signed the school’s Acceptable Use of the Internet Policy for staff;
* report any suspected misuse or problem to the school’s online safety co-ordinator;

**Professional Development of Staff:**

Teachers are the first line of defence in online safety. Our observation of behaviour is essential in recognizing concerns about pupils and in developing trust so that issues are reported. Online Safety training is an essential element of staff induction and should be part of on-going Continuous Professional Development programme. Through this policy, we aim to ensure that all reasonable actions are taken and measures put in place to protect all users. All staff will receive regular information and training on Online Safety issues through the ICT coordinator at staff meetings. All staff must be made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

**Cyber Bullying:**

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communications both in and out of school. This form of bullying is also referenced to within our school’s overall Anti-Bullying and Pastoral Care Policies. 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. It is important that pupils are encouraged to report incidents to both school and, if appropriate, to the PSNI to ensure the matter is properly addressed and the behaviour ceases. We will also keep a record of cyber-bullying incidents to monitor the effectiveness of our preventative activities and to review and ensure consistency in our investigations, support and sanctions.

**Communication of our Online Policy:**

This policy, supported by the school’s Acceptable Use Agreement for staff, pupils and visitors, is to protect the interests and safety of the whole school community. All teachers and parents have received a copy and thereafter parents of Year 1 will receive a copy included in their welcome pack. A copy of the policy will also be available on the school’s website. This policy and its implementation will be updated on a regular basis.

Online safety rules will be discussed in all classrooms at the beginning of every academic year. Lessons from the whole school programme will be delivered at relevant times throughout the year and feedback provided during staff meetings. Parents/Carers are asked to read through and sign the acceptable use agreement on behalf of their child. The school’s website also provides links to sites highlighting online safety issues.

**Internet Security:**

Staff and pupils accessing the internet via the c2k network will be required to authenticate using their c2k username and password which provides filtering via the c2k education network solution. Access to the internet will be supervised at all times. Access via the c2k network is also fully auditable and reports are available to the school principal.

**Safer Schools App**

The school has created a Safer Schools App account. This has been shared with parents/carers and staff to provide regular safety updates and information.

**Policy for the use of Photography and Videos**

The purpose of this policy is to set out the school’s position in relation to use of photography and video in school by both staff and parents.

**Rationale**

At St. Joseph’s Primary School, we welcome positive publicity. Photographs and video clips add colour, life and interest to school activities and initiatives and help the school community to identify and celebrate the school’s achievements. We believe that parents have the right to record memorable moments within their children’s school lives in photographs and/or video, where appropriate. In deciding whether or not it is appropriate to allow the use of photography and/or video it is important to ensure the protection of the children in our care. There are occasions where it would not be appropriate for photographs to be taken of children in school, for example, when swimming or getting changed before or after a performance. It is therefore important that there are clear guidelines for the taking of images.

***The use of the word ‘images’ in this policy applies to both photography and video, although, in most cases only photographs are used.***

**Opportunities for Photography/Videoing**

There are many times in the school year when photography is used, including:

• Performances and events (e.g. Christmas, sports day, St. Patrick’s Day)

• ‘Special days’ (e.g. Grandparent’s Day, Super Learning days)

• School trips and outings

• Special occasions (school celebrations and parties, e.g. Graduation, sacramental services)

• Professional individual and class/school photographs

• For the School Prospectus

• To display within the school

• For press releases

• For the school website/LNI

• As a record of teaching and learning experiences.

**The Use of Images**

There are different ways in which these images will be used, for example:

• Images taken and used personally by parents

• Images which may be displayed in and around the school

• Images which will be shared with others in the school community

• Images which are available to a wider audience

This policy intends to clarify arrangements for the use of images and consent required in each of these circumstances.

**Parents’ use of images**

When parents attend events and performances within school, they may take photographs of their children for their own use. Photography/videoing will not be permitted in areas where children are changing into costumes/PE kits etc.

**Use of images within school**

Parental permission will be sought through a consent form completed on admission to the school in Primary 1 or in subsequent years for the use of photographic/video images within the school (see Appendix 3). Such images will only be displayed inside the school building. It is important to note that this category includes professionally taken class group photographs.

**Sharing images with the school community**

This includes images used within school publications such as school newsletters, to share information/celebrations with parents of children in the school. Parental permission will be given through the consent form completed, for the use of images in these circumstances. Personal information, such as names, will not be included unless permission has been sought separately.

**Sharing images with a wider audience**

Images placed on the school website and photographs used within the press will only be used where it is of benefit to the school, e.g. in demonstrating an aspect of the school which is most effectively displayed with children in the picture. Examples of this might be: publicising school successes such as winning an award; showcasing events such as performances; and for visits made to the school by ‘VIPs’ such as the local MP or celebrities. Parental permission for such images will be through the admissions consent form unless personal information, such as pupil names, are to be used, in which case permission will be sought separately.

**Parental Consent**

Parents of children attending the school will be asked to complete a consent form upon admission. This consent will be valid for the time the child attends the school.

Once consent has been received, the school will use images as permitted within this policy. No further consent will be sought by the school unless requesting permission to include a child’s name, e.g. in a newspaper article. Parents may change their consent options at any time by requesting a new form and completing it as appropriate.

**Responsibilities**

The Principal is responsible for ensuring that images are used as set out in this policy with appropriate consent from parents, providing reminders as stated.

Parents are responsible for ensuring that images are used responsibly and are not published in the press without consent from the school.

*Please note - The school does not accept liability for parents who do not adhere to such requests.*

**Monitoring**

Staff and Governors will review this policy every two years, taking into account advice and guidelines provided by local or national Government.

The Principal will monitor the implementation of this policy and will ensure that all staff are aware of its contents. Procedures set out within this policy will be maintained until the policy is reviewed. Any changes made to this policy will be communicated to parents as necessary.

**Social Networking Policy for all staff, governors and**

**volunteers at St. Joseph’s Primary School**

Social networking activities conducted online outside work, such as blogging involvement in social networking sites such as Facebook, Twitter, etc. and posting material, images or comments on sites such as You Tube, can have a negative effect on an organisation’s reputation or image. In addition, St. Joseph’s Primary School has a firm commitment to safeguarding individuals in all aspects of its work. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

**Key Principles**

* Everyone at St. Joseph’s Primary School has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.
* It is important to protect everyone at St. Joseph’s from allegations and misinterpretations which can arise from the use of social networking sites.
* Safeguarding children is a key responsibility of all members of staff and it is essential that everyone at St. Joseph’s considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.
* This policy relates to social networking outside work (as part of our contract with C2K, sites such as Facebook and Twitter are blocked automatically). Blogging and accessing social networking sites at work using school equipment is not permitted.
* No communications, irrespective of their anonymity should be shared that relate to any specific event, pupil or person at St. Joseph’s Primary School.
* To set out the key principles and code of conduct expected of all members of staff, governors, friends and volunteers at St. Joseph’s Primary School with respect to social networking.
* School staff will not invite, accept or engage in communications with

 parents or children from the school community to any personal social

 networking sites while in employment at St. Joseph’s Primary School.

* Any communication received from children to must be reported to the Principal or designated Child Protection officer and procedures for safeguarding followed.

**Code of Conduct**

The following are **not considered acceptable** at St. Joseph’s Primary School:

* The use of the school’s name, logo, or any other published material without written prior permission from the Principal or Vice Principal. This applies to any published material including the internet or written documentation.
* The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
* The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
* The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

**In addition to the above everyone at St. Joseph’s Primary School must ensure that they:**

* Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.
* Use social networking sites responsibly and ensure that neither their personal, professional or school’s reputation is compromised by inappropriate postings.
* Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

**Potential and Actual Breaches of the Code of Conduct**

In instances where there has been a breach of the above Code of Conduct, the following will apply:

* Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school’s ethos and principles.
* The Board of Governors will take appropriate action in order to protect the school’s reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

\*In the context of this policy “everyone” refers to all members of staff, governors and anyone working in a voluntary capacity at the school

**Use of Twitter & Facebook**

**Aims of Using Social Media:**

* **To quickly share and celebrate children’s achievements, successes and school updates.**
* **To demonstrate safe and responsible use of social media**
* **To encourage the use of 21st Century technology**

**Rationale**

The rationale of this policy is to explain acceptable use of Twitter and Facebook relating to St Joseph’s Primary School for staff, children, parents and governors. The policy will therefore aim to explain the purpose of Twitter and Facebook in St Joseph’s Primary School and the benefits that will arise from its proper use, and also deal with any potential pitfalls from using a web2.0 technology.

**Who controls content for St. Joseph’s Primary School.**

The uploading of content for St. Joseph’s Primary School will be controlled by members of the Senior Leadership Team. They alone will be responsible for password protection and uploading of content.

**Who can follow St. Joseph’s Primary School.**

*When* St. Joseph’s Primary Schoolreceives *a follow request it will make informed decisions on a case-by-case basis as to accept or decline. These decisions will be based upon a number of factors:*

* The name of the individual as read on their Twitter account and whether this name correlates to that of a parent on the SIMS database; is a member of staff; is a school governor; is a known and proper person to the SLT or ICT Leader;
* The quality of the biography of each individual as read in the bio section of their Twitter account;
* The images on view in the potential followers Twitter account.

In most cases, one or more of the above will be enough to accept a follow request. In the unlikely event that a parent or other suitable follower is inadvertently rejected, the SLT will hear each individual on a case-by-case basis. These hearings will usually involve the prospective follower making themselves known in person to the above named persons, with their Twitter details, and should take no more than a few minutes**.**

**Who will St. Joseph’s Primary School follow? (Twitter)**

In order to protect itself from inappropriate content being distributed into its news feed, will be selective in who we seek to follow. We will only seek to follow those **@StJosephsAntrim** whose @ handle has obvious benefits to the school. Once again, these will be decided on a case-by-case basis at the discretion of the SLT.

**@StJosephsAntrim** **sees itself more as a distributor of information to those who follow it and not as a receiver of information.**

**What is inappropriate content and referencing and how will it be dealt with?**

St. Joseph’s Primary Schoolwelcomes any referencing, mentions, or interactions that promote the school in a positive light only.

Therefore, St Joseph’s Antrim PS deems any of the following as inappropriate:

* Offensive language or remarks aimed at the school, its staff, parents, governors or others affiliated with the school;
* Unsuitable images or content posted into its feed;
* Unsuitable images or content finding its way from another’s account into the **@StJosephsAntrim** feed.
* Images or text that infringe upon copyright;
* Comments that aim to undermine the school, its staff, parents, governors or others affiliated with the school.

Any inappropriate content will be deleted and its users will be removed, blocked, and, depending on the nature of the comment, reported.

Appendix 1

**E-Safety Agreement**

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

* On the network, I will only use my own login username and password.
* I will keep my username and password private.
* I will not access other people’s files without their permission.
* I will not change or delete other people’s work/files.
* I will ask permission before entering any website, unless my teacher has already approved that site.
* I will use the Internet for research and school purposes only.
* I will only send e-mail (KS2 Only) which my teacher has approved. I will make sure that the messages I send are polite and responsible.
* I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
* When sending e-mail (KS2 Only) I will not give my name, address or phone number or arrange to meet anyone.
* I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
* If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
* I will not bring in memory sticks or any other memory devices from home to use in school unless I have been given permission by my class teacher.
* I understand that the school may check my computer files/emails and may monitor the Internet sites that I visit.

**I know that if I deliberately break these rules my Internet privileges will be suspended and my parents/cares will be informed.**

 **Pupil Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_

As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including e-mail (senior classes). I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.

**Parent/Carer Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Appendix 3

**St. Joseph’s Primary School**

PARENTAL CONSENT

Use of Photographs

**Please delete or circle where appropriate:**

**Name of Child: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

I **do** / **do not** give my consent to photographs being taken of my child to be used in displays in school.

I **do** / **do not** give my consent to having my child in any school/class/group photographs for any newspaper/school newsletter.

I **do** / **do not** give my consent to my child taking part in any school/class videos.

I **do** / **do not** give my consent to my child taking part in any school/class performances.

I **do** / **do not** give my consent to my child being involved in any picture/videos of school activities that will be available to view through the school website and/or Seesaw and/or school Facebook page and/or school Twitter page.

Person(s) with parental responsibility please sign below

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Appendix 2

**Online Incident Register**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date:**  | **Incident details**  | **Pupil Name**  | **Staff Involved**  | **Action / Resolution**  |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |