St. James the Great Roman Catholic Primary and Nursery School

E-Safety Policy

Date Created: Autumn 2012
Date Reviewed: Autumn 2013

Rationale

From St. James the Great Mission Statement:

"…the school will provide a framework within which all pupils are enabled to develop the highest possible level of achievement, fulfilling their academic, moral, physical and spiritual potential."

Aims and Objectives

ICT has an all-encompassing role within the lives of children and adults. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging often using simple web cams
- Blogs
- Podcasting
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones

The use of such technology greatly enhance communication and the sharing of information and at St. James the Great, pupils and staff are to be encouraged to use them in a positive and responsible way. However, their use can put young people at risk within and outside of school. Some of these dangers include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of/ sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing /distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/ internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document has been drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks.

Roles and Responsibilities

This Policy applies to all pupils, parents and carers, teaching and support staff, governors, volunteers, students and visitors. This list is not to be considered exhaustive.

The Role of the Designated Person/s for Child Protection

- To attend training in e-safety issues and be aware of the potential for serious child protections issues to arise from:
    - Sharing of personal data.
    - Access to illegal/ inappropriate materials.
    - Inappropriate on-line contact with adults/ strangers.
    - Potential or actual incidents of grooming.
    - Cyber-bullying.
- To provide support and advice to staff as regards potential e-safety issues.
- To liaise with the ICT Subject Leader and other staff in regards to the implementation and monitoring of the E-safety programme of work.
- To update the Head teacher and Governors of any e-safety issues that need attention.

The Role of Teaching and Support Staff

- To have an up-to-date awareness of e-safety matters and of the current school policy and practices related to e-safety.
- To report any suspected misuse or problem to the Designated Person/s for Child Protection for investigation/ action/ sanction.
- To ensure any digital communications with pupils are on a professional level and only carried out using the official school systems.
- To ensure personal information including telephone contact details are not provided to pupils.
- To carry out the school's E-safety programme of work is and imbed in everyday practice in all aspects of the curriculum.
- To ensure pupils understand and follow the e-safety rules (see Appendix 2). A copy should be easily accessible to the pupils e.g. displayed in the classroom. Copies should be signed as appropriate for the age and understanding of the pupils.
- To ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- To monitor ICT activity in lessons and extra-curricular/ extended school activities as appropriate.
- To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices which should not be within the children's possession in school.
- To ensure that in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with unsuitable material that is found in Internet searches.
- To understanding the contents of this Policy and other e-safety related policies, and to sign the Staff E-Safety Agreement Form (Appendix 5).

The Role of Pupils

- To abide by the school's rules for safe Internet Use.
- To avoid plagiarism and uphold copyright regulations.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- To abide by the school's policy as regards the use of mobile phones, cameras and other digital devices.
- To understand and abide by the school's anti-bullying policy.
- To understand the importance of adopting good e-safety practices outside of school.

The Role of Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/ mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parent evenings, newsletters, letters, website, e-safety campaigns or literature (Appendix 3**).** Parent/ carers should understand the contents of this policy and sign the E-Safety Agreement Form (Appendix 4).

Curriculum

The school follows an E-Safety programme of work (Appendix 6) based in a large part on the resources available from the Think U Know website (www.thinkuknow.co.uk). One ICT lesson every term is dedicated to teaching pupils about e-safety, although the teaching of e-safety awareness is embedded in all use of technology across the curriculum.

Use of Digital and Video Images

Examples of how digital photography and video may be used within school include:

- Pupils being photographed (by the classroom teacher, teaching assistant or another pupil) as part of a learning activity e.g. photographing pupils at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the pupils to see their

work and make improvements.

- A pupil's image for presentation purposes around the school e.g. in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson.

- A pupil's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, a pupil's image could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If a circumstance arose where the school wanted to link a pupil's image to their name e.g. if the pupil won a national competition and wanted to be named in local or government literature, parents would be contacted separately for permission.

The following safeguarding principles are followed with specific regard to the use of digital and video images:

- The school gains parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- Only images of pupils in suitable dress are used.
- Parents volunteering on class trips are not allowed to take photographs or videos on their personal equipment.
- Digital images /video of pupils are stored in a private teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a subject leader/ school documentation.
- The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their eSafety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Website:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorizers.
- The school web site complies with the school's guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, stjamesthegreat@stjamesthegreat.org.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

Next Policy Review Date: Autumn 2014

Linked Policies

Anti-bullying
Discipline and Behaviour
Child Protection
ICT

APPENDIX 1

Our Internet Rules

We developed the following rules to ensure the privacy and safety of pupils when using the Internet & W.W.W. Please understand them.

- Children are only referred to by first names on our web pages.
- Any images of children will not be labeled with their names.
- No close up pictures of our children will be available online.
- Children and staff will never reveal their personal details, and home addresses & telephone numbers on the web or in dialogue with other Internet users.
- All E-mail to classes will be moderated by the class teacher.
- Children will not engage in conversation or dialogue with other users on the Internet without permission or supervision from their teacher.
- Children are only allowed to use the provided links by themselves. The free use of Search Engines, is not permitted, unless in the presence of a teacher or other adult in school.
- The Search Engines used by children at St. James all offer a filtered list of links.
- Any child finding themselves uncomfortable or upset by anything they discover on the Internet will report it to a teacher immediately.
- Downloading of files is restricted to staff, or children under supervision.
- Children have no access to Newsgroups.
- All Internet access at St. James the Great Primary School is filtered through a proxy server to screen undesirable sites at source - this facility must only be disabled by the ICT coordinator.
- In the interests of security, St. James the Great Primary School reserves the right to make a detailed log of your access to any site, including your Internet Service Provider and details of your computer system.

A note to parents:-

The school recognizes that, under certain circumstances, the Internet can give children access to undesirable information and images. We have done all that is possible to ensure children are protected from such information through the use of security software, limiting of features and the construction of an Intranet and Web site that provide as safe an environment as possible. The children are taught to use the facility sensibly and with proper consideration for others.

It is recommended that parents using the Internet at home with children, develop a similar set of rules and install appropriate security software.

APPENDIX 2

Our Internet Rules – FS, KS1, KS2

St. James the Great School Rules for Responsible ICT Use

I will only use the Internet with an adult.

If I see something I don't like on a screen, I will tell an adult.

These rules will help to keep everyone safe and help us to be fair to others.
My teacher has explained what these rules mean.

Name:

St. James the Great School Rules for Responsible ICT Use

I will only send polite and friendly messages.

I will only use the Internet and email with an adult.

If I see something I don't like on a screen, I will tell an adult.

I will only click on icons and links when I know they are safe.

My teacher has explained what these rules mean.

Name:

St. James the Great School Rules for Responsible ICT Use

- ☺ I will only use the school's computers for schoolwork and homework.
- ☺ I will only delete my own files and not look at other people's computer files without their permission.
- ☺ I will keep my login and password secret.
- ☺ I will not bring computer files into school without permission.
- ☺ I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- ☺ I will only e-mail people I know, or my teacher has approved, and will never add hyperlinks to my email.
- ☺ The messages I send, or information I upload, will always be polite and sensible.
- ☺ I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- ☺ I will not give my home address, phone number, send a photograph or video, or give out any other personal information.
- ☺ I will never arrange to meet someone I have only ever met on the Internet or by email or in a chat room.
- ☺ If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

My teacher has read the rules to me and explained what they mean. I agree that I will keep to them.

Signed……. Date……

APPENDIX 3

E-safety Leaflet for Parents and Carers

The best way to keep your child safe when using the internet is to talk to them and make sure they understand these simple rules.

NICKNAME Never give out personal details to online 'friends'. Use a nickname when logging on and don't share full name, email address, mobile number, school name or any photos.

FAMILY ROOM Talk to your child about what they are doing online and who they are talking to. Get them to show you how to use things you are not familiar with. Keeping the computer in a family room means that you can share your child's online experience, they are less likely to act inappropriately (i.e. via webcam) and their online 'friends' will see they are in a family room.

UPSET If your child receives a message that upsets them, remind them not to reply, they should save the message and show you or another trusted adult.

STRANGERS Don't open files sent from people you don't know. They could contain a virus, or worse – an inappropriate image or film. An online 'friend' is anyone you have not met in real life; no matter how long you have been friends with them.

LIES Help your child to understand that some people lie online and that it's better to keep online 'mates' online. They should never meet up with any online 'friends' without an adult they trust. Spam and junk emails and texts are not true, don't reply or send them to anyone else, just delete them.

BLOCK Make sure they know how to block someone online and report them if they feel uncomfortable.

FACEBOOK Did you know that it is against site regulations for a child under the age of 13 to have a Facebook account? As all children at St. James the Great are below the age of 13, no child should have access to this.

BLAME Make sure your child feels able to talk to you, let them know that it's never too late to tell someone if something makes them feel uncomfortable. Don't blame your child, let then know you trust them.

APPENDIX 4

Parent/Carer E-Safety Agreement Form

Parent /Carer name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, e-mail and other ICT facilities at school.

I know that my daughter or son has been made aware of the School Rules for Internet Use (Appendix 2).

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Use of digital images - photography and video
I also agree to the school using photographs of my child or including them in video material, as described in this policy. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent /Carer signature: _____ Date__/__/__

APPENDIX 5

Staff E-Safety Agreement Form

This covers use of digital technologies in St. James the Great including email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Designated Persons for Safeguarding.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access any of the school's systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the school email system for any email communication related to work at St James the Great.
- I will only use other school approved communication systems for any communication with young people or parents/carers.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Designated Persons for Safeguarding who are Mr Stephen Beck, Miss Lavinia Spong or Mrs Tammy Scott Cree.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.
- I will not use personal digital cameras or camera phones for taking and transferring images of young people or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role. I understand that it is my responsibility to ensure I know how to use any such tools so as not to compromise my professional role, such as setting appropriate security settings.

- I agree and accept that any computer or laptop loaned to me by St. James the Great, is provided solely to support my professional responsibilities and that I will notify the Designated Persons for Safeguarding of any "significant personal use".
- I will access school resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is kept securely.
- I understand that data protection policy requires that any information seen by me with regard to service users, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand that it is my duty to support a whole organisation safeguarding approach and I will alert the Designated Persons for Safeguarding if I feel the behaviour of any service user or member of staff may be **a cause** for concern or inappropriate.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to the Headteacher on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User's Name: _____

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet/ Internet and be able to use the school's ICT resources and systems.

User's Signature: _____ **Date**___/___/__

APPENDIX 6

Overview of E-Safety Programme of Work

	Autumn	Spring	Summer
Reception	1. Children are aware that they can use the Internet to play and learn, supported by a trusted adult/teacher. 2. Children begin to understand the difference between real and online experiences.	1. For children to understand the importance of politeness and courtesy on and off the internet.	1. To reinforce the message of 'Stranger Danger' on the internet. 2. For children to know what action to take if they feel they are in danger.
Year 1	1. Children understand that some information about themselves is special because it makes them unique. 2. Children know that they should never give out their personal details online without a parent or teacher's permission.	1. Children understand that not everyone they meet is automatically trustworthy. 2. Children begin to identify the characteristics of people that are worthy of their trust and who can help them make positive choices to keep them safe.	1. Children begin to understand some of the qualities that can be used to assess if a person is trustworthy. 2. Children can identify situations in which it is wise to turn to a trusted adult for help.
Year 2	1. Children understand that their emotions can be a powerful tool to help them assess unsafe situations. 2. Children can identify some of the physical sensations that alert us to unsafe situations.	1. Children understand the importance of checking with an adult before participating in the online environment. 2. Children feel encouraged to be open about their online experiences with a trusted adult.	1. Children understand that actions that may be seen as a joke by some can be hurtful to others. 2. Children begin to understand the feelings of someone who is teased or bullied.
Year 3	1. To understand that the Internet is used for a very wide range of purposes. 2. To recognise that not all websites provide true information.	1. To understand the concept of personal information. 2. To know when it is safe and unsafe to provide personal information.	1. To recognise the different risks in different situations and then decide how to behave responsibly.
Year 4	1. To know how to respond to cyber bullying.	1. To be able to evaluate information from the internet.	1. To understand the potential risks associated with divulging personal information to people they do not know, especially people they have met online.
Year 5	1. To develop an awareness of the potential dangers of using mobile phones. 2. To be able to take appropriate action.	1. To be aware of the potential impact of cyberbullying and help them reflect on their own online behaviours.	1. To know some strategies to deal with difficult situations when using technology.
Year 6	1. To be able to stay safe when using a social network.	1. To be able to stay safe when using a social network.	1. To use social networks responsibly. 2. To know how to stay safe in an online environment.