St Mary’s Catholic First School
E-Safety Policy

In reviewing this policy and making decisions regarding e-safety due consideration has been given to Equality Legislation.

St. Mary’s e-Safety co-ordinator is Paula Fearn
St. Mary’s e-safety Governor is Rich Elliott

Our e-Safety Policy has been written by the school, drawing on current government guidance. It has been agreed by senior management and approved by the governors. The e-Safety Policy and its implementation will be reviewed annually.

1. Teaching and Learning

1.1 Why the internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2 Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and effective curriculum practice;
- communication and collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA;
- access to learning wherever and whenever convenient.

1.3 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils will be shown how to publish and present information to a wider audience.

1.4 Evaluation of Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross checking information before accepting its accuracy.

2. Managing Internet Access

2.1 Information system security

- School ICT systems security will be reviewed regularly by DCC IT Support
- Virus protection will be updated regularly by DCC IT Support
- Portable media, such as memory sticks and CD-ROMs, may not be used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

2.2 E-mail

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects. However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, e-mail is not considered private and is monitored by staff, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Whole-class or group e-mail addresses are used at Key Stage 2 and below.
- Pupils may not access personal email accounts in school.
- E-mail sent to an external organisation is written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- The sending of abusive or inappropriate email messages is forbidden.

2.3 Published content and the school website

The school web site – www.stmarysdorchester.dorset.sch.uk celebrates pupils' work and promotes the school.

- The point of contact on the Web site is the school address, school e-mail and telephone number. Staff or pupils' personal information is not published.

- The Headteacher and ICT Co-ordinator take overall editorial responsibility and try to ensure that content is accurate and appropriate.

2.4 Publishing pupil's images and work

- Photographs that include pupils are selected carefully so that individual pupils cannot be identified and their image misused. Consider using group photographs rather than full face photos of individual children.
- Pupils' full names are not used anywhere on the Web site or other online space, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are electronically published (see APPENDIX 1).
- Work can only be published with the permission of the pupil and parents/carers.
- The copyright of all material is held by the school, or is attributed to the owner where permission to reproduce has been obtained.
- Pupil image file names will not refer to the pupil by name.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.5 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

2.6 Managing filtering

- The school works in partnership with parents, the LA, and SWGfL to ensure that systems to protect pupils are reviewed and improved.
- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as the Internet Watch Foundation (IWF) or CEOP: Child Exploitation and Online Protection Centre.

2.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior management team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

2.8 Protecting personal data

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

3. Policy Decisions

3.1 Authorising Internet access

- The school allocates Internet access for staff and pupils on the basis of educational need. Parental permission is required for each pupil.
- All staff must read and sign the 'Acceptable use rules for staff' statement before using any school ICT resource (see APPENDIX 3).
- Parents will be asked to sign an ICT acceptable use form (see APPENDIX 1) along with a form about publishing/ taking photographs (see APPENDIX 2).
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Key Stage 2, pupils accessing the internet are directly supervised by a member of staff.
- Any person not directly employed by the school will be asked to sign the 'Acceptable use Rules for Staff' statement (see APPENDIX 3) before being allowed to access the internet from the school site.

3.2 Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor SWGfL can accept liability for any material accessed, or any consequences of Internet access.

Methods to identify, assess and minimise risks will be reviewed regularly. The headteacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

3.3 Complaints procedures

- Prompt action is required if a complaint regarding the inappropriate use of the Internet is made. The facts of the case need to be established, for instance whether the Internet use was within or outside school.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.

- Complaints of a child protection nature must be referred the school Designated Safeguarding Leader and dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of consequences for pupils misusing the Internet. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions are in place, linked to the school's behaviour policy.
- Sanctions available include:
    - interview/counselling by Headteacher
    - informing parents or carers
    - removal of internet or computer access for a period.
- Pupils and parents will be informed that any complaint will be treated sensitively and seriously
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with other safeguarding issues, there may be occasions when the police must be contacted.

4. Communications Policy

4.1 Introducing the e-Safety policy to pupils

- E-Safety rules will discussed with the pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety is in place, including whole-school and class-based workshops and discussions with members of the Dorset's e-Safety team.
- Instruction in responsible and safe use will precede Internet access.
- e-Safety training will be embedded within the ICT scheme of work for all subjects of the curriculum.

4.2 Staff and the e-Safety policy

- All staff will be given the e-Safety policy and its application and importance explained.
- Staff should be aware that network and Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff will use a child friendly safe search engine when accessing the web with pupils.
- Regular e-Safety training will be provided in conjunction with the Dorset e-Safety team.

4.3 Enlisting parent/carer support

Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate, supervised use of the Internet at home. Parents are also advised to check if pupils' use elsewhere, such as libraries, is covered by an appropriate use policy.

- Parents'/Carers' attention will be drawn to the school's e-safety Policy in newsletters, the school brochure and on the school website.

- Events to highlight e-Safety will be organised regularly in conjunction with Dorset’s e-Safety team and will be open to parents of children attending other local schools
- Internet issues will be handled sensitively, and parents/carers will be advised accordingly.
- A partnership approach with parents will be encouraged.
- The school will maintain a list of e-Safety resources for parents/carers.
- The school will ask new parents to sign the parent/pupil agreement when they register their child within the school (see APPENDIX 1)

Adopted by Full Governing Body Date: ***14th December 2016***

Review date: ***December 2017***

Signed:

APPENDIX 1

Our School
e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil: ***Form:***

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed: ***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: ***Date:***

Please print name:

Please complete, sign and return to the school secretary

Key Stage 1

Think then Click

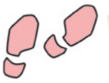
These rules help us to stay safe on the Internet

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.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- ***We ask permission before using the Internet.***
- ***We only use websites that an adult has chosen.***
- ***We tell an adult if we see anything we are uncomfortable with.***
- ***We immediately close any webpage we not sure about.***
- ***We only e-mail people an adult has approved.***
- ***We send e-mails that are polite and friendly.***
- ***We never give out personal information or passwords.***
- ***We never arrange to meet anyone we don’t know.***
- ***We do not open e-mails sent by anyone we don’t know.***
- ***We do not use Internet chat rooms.***

APPENDIX 2

Parent consent form for use of pupil images

At **St. Mary's** we take the issue of child safety very seriously, and this includes the use of images of pupils. Including images of pupils in school publications and on the school website can be motivating for the pupils involved, and provide a good opportunity to promote the work of the school. However, schools have a duty of care towards pupils, which means that pupils must remain unidentifiable, reducing the risk of inappropriate contact, if images are used in this way.

We ask that parents' consent to the school taking and using photographs and images of their children. Any use of pupil images at **St. Mary's** is underpinned by our school's acceptable use internet policy. We will never include the full name of the pupil alongside an image.

Please complete, sign and return this form to **Paula Fearn** at **St. Mary's**

I **agree/do not agree** to photographs and digital images of the child named below, appearing in **St. Mary's** printed publications or on the school website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed by other media, such as CD-ROM, as part of the promotional activities of the school

Name of child: ....

Name of parent or guardian: ....

Address: ....

....

....

Signature: ....

Date: ....

APPENDIX 3

Acceptable Use Rules for Staff

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children’s or young people’s safety to the Headteacher, Designated Safeguarding Leader or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Safeguarding Leader is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child’s school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for inappropriate personal use.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install approved hardware and software for which I have been given permission.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with Mrs Linda Lake.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed………………………………………………….Date…………………… Name (printed)…………………………………………………

School……………………………………………………………………………..