St Mary Federation E-Safety Policy

This policy sets out clearly our expectations on pupils, staff, parents and members of the wider community to ensure best practice.

Writing and reviewing the E-safety policy

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

- The schools will identify a member of staff who has an overview of E-safety, this would usually be the Senior Designated Professional (SDP). The current member of staff is Mrs Sarah Bocking, Head Teacher.
- Our E-safety Policy has been written by the schools, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The E-safety Policy and its implementation will be reviewed annually
- It was approved by the Governors on: 19th June 2013
- The E-safety Policy was discussed by Staff on: 19th June 2013
- The E-safety Policy was discussed by a parent committee on 16th May 2013
- The E-safety Policy was discussed by the School Council on: 18th May 2013
- The E-safety Policy was revised by the curriculum committee on 29th January 2014
- And reviewed again 27/1/15 by curriculum committee
- Reviewed and adopted for the Federation at the SVC committee 18th January 2016

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st Century life for education, business and social interaction. It is an open communications channel allowing information to be transmitted to many locations in the world. Messages may be sent, ideas discussed and material published, with very little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

➢ Each school has a duty to provide students with quality Internet access as part of their learning experience.

➢ Internet use is a part of the curriculum and a necessary tool for staff and pupils.

The purpose of Internet use in school

To promote pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration systems.

Benefits of using the Internet in education include:

- Access to world-wide educational resources
- Inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC)
- Educational and cultural exchanges between pupils world-wide
- Cultural, 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 good curriculum practice
- Communication with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks
- Exchange of curriculum and administration data with the LEA and DfES.

➢ The school Internet access is provided by Norfolk County Council, ICT solutions, and includes 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

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

Pupils will be taught how to evaluate Internet content

- The schools will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority

E-mail

- **Pupils and staff may only use approved e-mail accounts on the school system.**
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The schools will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

- Sarah Bocking and office staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing photographs, images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The Federation may wish to use group photographs rather than full-face photos of individual children.

- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs or images of pupils are published

- Written permission from adults will be obtained before their names, photographs or images of themselves are published

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing on the school learning platform

- The schools will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.

- Newsgroups will be blocked unless a specific use is approved.

- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

- Pupils must not place personal photos on any social network space provided in the school learning platform without permission.

- Pupils, parents and staff will be advised on the safe use of social network spaces

- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The schools will work in partnership with Norfolk Children's Services to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff.
- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet **(1)**.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

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.

Other devices

- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. Taking photographs at any time without the subject's consent will be discouraged.
- The sending of abusive, offensive or inappropriate material is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.
- Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

Protecting personal data

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

(1 This is under review)

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents will be asked to sign and return a consent form.
- **Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access.**
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the Internet on the school site.

Assessing risks

- The schools will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.
  The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be referred to the Senior Designated Professionals for Safeguarding and dealt with in accordance with school child protection procedures.
- The senior designated professional for Safeguarding is Mrs Sarah Bocking, head Teacher: head@brancaster.norfolk.sch.uk 01485 210246
- The alternate designated professionals for Safeguarding are clearly identified within each school on posters and leaflets available at Reception.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

Staff and the E-safety policy

- All staff will be given the School E-safety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- **Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.**

Enlisting parents' support

- Parents' and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Appendix 1:

Staff, Governor and Visitor – ICT Code of Conduct

St Mary Federation

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This code of conduct is provided to ensure that all users are aware of their responsibilities when using any form of ICT provided by or directed by Norfolk County Council. All such users will be issued with this code of conduct. Any concerns or clarification should be discussed with ***Mrs Sarah Bocking, Head Teacher***

- All staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, laptops and tablets

- All staff, Governors and visitors understand that it is a disciplinary offence to use the school ICT system and equipment for any purpose not permitted by its owner.
  (Teaching Staff http://www.schoolspeoplenet.norfolk.gov.uk/Teaching-Staff/Working-in-a-Norfolk-School/Resolving-Issues/Disciplinary/index.htm
  Support Staff http://www.schoolspeoplenet.norfolk.gov.uk/Support-Staff/Working-in-a-Norfolk-school/Resolving-Issues/Disciplinary/index.htm)

- All staff, Governors and visitors will not disclose any passwords provided to them by the school or other related authorities.

- All staff, Governors and visitors understand that they are responsible for all activity carried out under their username

- Staff, Governors and visitors will not install any hardware or software on any school owned device without the permission of ***Mrs Sarah Bocking, Head Teacher***

- All staff, Governors and visitors understand that their permitted use of the Internet and other related technologies is monitored and logged and will be made available, on request, to their Line Manager or Head teacher in line with any disciplinary procedures. This relates to all school owned devices, including laptops provided by the school.

- All staff, Governors and visitors will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted by the Head or Governing Body.

- All staff, Governors and visitors will ensure that all their school generated electronic communications are appropriate and compatible with their role.

- All staff, Governors and visitors will ensure that all data is kept secure and is used appropriately as authorized by the Head teacher or Governing Body. If in doubt they will seek clarification. This includes taking data off site.

- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- All staff, Governors and visitors will only use the approved email system(s) for any school business

- Images will only be taken, stored and used for purposes in line with school policy. Images will not be distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Head teacher.

- All staff, Governors and visitors will comply with copyright and intellectual property rights.

- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Senior Designated Professional or Head teacher in line with the school's Safeguarding Policy.

I acknowledge that I have received a copy of the ICT Code of Conduct.

Full name:……(printed)

Job title:……

Signature:……**Date:**……

Appendix 2:

Internet safety rules

1. I will ask before I go on a game
2. I will use my own log in
3. I will not get rid of other people's work
4. I will ask before using something from home on the computer
5. I won't use emails without the teacher being there
6. I won't use facebook
7. I will tell the teacher if I see something that I don't think is right
8. If I get lost on the internet, I will ask for help
9. I will never give out personal information or passwords
10. I know the teachers can check what I'm doing and if I do something wrong my teacher will stop me from using the internet

Pupil name: ……

Pupil signature:…… **Date:**……

Appendix 3: cover letter for parents

E-safety

Do your children know more about the internet and technology than you?
Do you always know what they are doing and what the possible dangers are?

The internet is now an everyday part of life and our children are often more active than we are. It is important that we all understand the possible dangers and know how to keep safe.

Did you know…

- Half of all children have experienced cyber bullying
- Half of all families have accidentally downloaded malicious software/ viruses
- 4 in 10 families say their child has accidentally cost them money through downloads/links
- 6 in 7 children have accidentally found inappropriate sites
- 1 in 7 children have been approached by online predators
- Inappropriate photos or text posted now can seriously affect job or university chances later in life

In order to keep children safe at school, we have written a new **e-safety policy**

Pupils will be taught to:

- Know and use safe websites and to be careful when following links
- Ask before using a new website or game
- Know how to report unpleasant/inappropriate content
- Keep safe by not giving out personal details or anything which would allow them to be identified or traced (eg a picture outside their home)
- Only use own log in and keep this secure
- Only use emails/texts with adult permission and keep content appropriate
- Understand copyright

Staff will:

- Teach children how to keep safe
- Ensure as best we can, that anything the children have access to is appropriate
- Report to County any unsuitable sites so that they can be blocked

- Ensure that all adults, including visitors, use the internet safely and appropriately
    - Be available to advise parents if required

Useful links for parents

http://www.bbc.co.uk/webwise/topics/safety-and-privacy/online-safety-for-parents

http://www.saferinternet.org.uk/advice-and-resources

Appendix 4: parental agreement

St Mary Federation E-safety Policy

Parent / guardian name:……..

Pupil name: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school.

I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the e-safety policy. I also understand that my son/daughter may be informed, if the rules have to be changed during the year. I know that the latest copy of the policy is available on the website or from the office and that staff can inform me where further advice about safe use of the Internet can be found

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 a filtered internet service, secure access to 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. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour.

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.

Parent's signature:…… **Date:**……

Appendix 5: letter for children

E-safety

Do you use the internet and mobile phones?
Do you always know what you are doing and what the possible dangers are?

Did you know…

- Half of all children say they have experienced cyber bullying
- Half of all families have accidentally downloaded things that have harmed their computer?

- 4 in 10 parents say their child has accidentally cost them money when using the computer
- 6 in 7 children have accidentally found inappropriate sites
- Inappropriate photos or text posted now can seriously affect your job or university chances later in life

In order to keep you safe at school, we have written a new **e-safety policy**

You will be taught to:

- Know and use safe websites and to be careful when following links
- Ask before using a new website or game
- Know how to report unpleasant/inappropriate content
- Keep safe by not giving out personal details or anything which would allow you to be identified or traced
- Only use own log in and keep this secure
- Only use emails/texts with adult permission and keep content appropriate
- Understand copyright

Staff will:

- Teach you how to keep safe
- Explain our internet safety rules
- Ensure as best we can, that anything you have access to is appropriate
- Ensure that all adults, including visitors, use the internet safely and appropriately
- Ask you to sign a copy of the rules to agree to use the internet safely

Appendix 6:

Use of Personal Devices in School by Students

Best Practice Guide

Before any personal device is allowed into school an Acceptable User Policy should be signed by both the student and the parent/carer. This should include:

- A disclaimer which states that if the device is used inappropriately outside of the lesson the school cannot be held responsible.
- A section which makes clear to parents there can be violations and other issues and that these will be dealt with in accordance with school policy.
- Give a tariff of consequences of misuse should there be an issue e.g. device confiscated until the end of the day.
- That the school accepts no liability for any damage to or loss of personal devices and should be covered by family insurance.
- Acceptance that monitoring systems may be actively used.

Ensure that before any device linked to the internet is used, that monitoring systems are fully active, if available.

Ensure teaching staff are aware students may bring in authorised personal devices and how these additional resources can be optimised in lessons.

Ensure students are aware they are able to use authorised personal devices in school and where necessary in which lessons they can use them.

Consider asking how many students might be interested in using personal devices in school. If a high take up is indicated, the school may wish to consider rolling out use gradually i.e. on a year by year basis.

Student's mobile phones are permitted on the understanding that they are to be used as directed by the teacher for learning opportunities.

Appendix 7:

The Legal Framework surrounding E-safety (01.11.09)

This section is designed to inform users of legal issues relevant to the use of electronic communications. The law is developing rapidly

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is committed as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Education and Inspections Act 2006, sections 90 and 91, provide statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. **Section 94** also gives schools the power to confiscate items from pupils as a disciplinary penalty. These powers may be particularly important when dealing with E-safety issues: online bullying may take place both inside and outside school, and this legislation gives schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the well-being and safety of others.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to

know that his course of conduct will cause the other so to fear on each of those occasions.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from abuse based on their race, nationality or ethnic background.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Sexual Offences Act 2003
A new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and then intentionally meet them or travel with intent to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document, which is available from this website
http://www.gmc-uk.org/sex_offences_act_2.pdf_48793788.pdf