



St Mary's CE Primary eSafety & Data Security Policy March 2017

Do everything in love



1 Corinthians 16:14

Reviewed May 2016

Presented to Governors:

St Mary's Church of England Primary School is a warm, friendly and welcoming Church school that provides high quality education for all its pupils. As a Church school we hold our Christian values at the heart of everything we do. These are: Love; Respect; Determination; Courage; Compassion; and Honesty.

It is very important to us that the children are happy and experience the best education possible. We value strong links and a close partnership between home, church and school and recognise the importance of trust and shared responsibility in education

eSafety and Data Security Policy for ICT Acceptable Use

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites

E-mail, Instant Messaging and chat rooms

Social Media, including Facebook and Twitter

Mobile/ Smart phones with text, video and/ or web functionality

Other mobile devices with web functionality

Gaming, especially online

Learning Platforms and Virtual Learning Environments

Blogs and Wikis

Podcasting

Video Broadcasting

Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At St Mary's CE Primary School, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and

beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies ("specified authorities" listed in Schedule 6 to the Act), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism" (Prevent Duty Guidance, *HM Government* 2015). All members of staff must have regard to this guidance when carrying out that duty

St Mary's CE Primary ensure that children are safe from terrorist and extremist material when accessing the internet in school. As with other online risks of harm, every teacher is aware of the risks posed by the online activity of extremist and terrorist groups. All staff undergoes Prevent training. Halton Borough Council provides St Mary's with web filtering to keep our children safe.

St Mary's CE Primary School

Pupil Acceptable Use Agreement / eSafety Rules

I will only use ICT in school for school purposes.

I will not tell other people my ICT passwords.

I will only open/delete my own files.

I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

I will not give out my own details such as my name, phone number or home address online.

I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

I will only use a laptop or computer when an adult has said I can.

I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.



St Mary's School

St. Marys Church of England Primary School

Castlefields Avenue South

Halton Runcorn

Cheshire WA7 2NR

Tel: 01928 565995

Fax 01928 569298

e-mail head.stmarys@halton.gov.uk

Website www.stmaryshalton.co.uk

Head Teacher Rachel Tainsh B.A. (Hons)
P.G.C.E

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies have become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact us.

Simon Owen
ICT Subject Leader

St Mary's CE Primary School

We have discussed this and(child name) agrees to follow the eSafety rules and to support the safe use of ICT at St Mary's CE Primary School.

Parent/ Carer Signature

Class Date

St Mary's CE Primary School

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

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

- I will only use the school's email / Internet / Website (Learning Platform) and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will ensure that personal data (such as data held on SIMs) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without permission of the Subject Leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken on school cameras, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

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

Signature Date

Full Name(printed)

Job title

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses.

Never interfere with any anti-virus software installed on school ICT equipment that you use

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The school is aware of the Becta guidelines found at

<http://tinyurl.com/76gj9xr>

(published Spring 2009, please note that this organisation was closed in 2011 but the guidance is still useful), the advice and guidance given by the Information Commissioner's Office (ICO)

http://www.ico.gov.uk/for_organisations/data_protection/security_measures.aspx

and the Local Authority guidance.

Security

The school gives staff access to the school website and Shared Drive with a unique username and password

- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed off through an authorised agency or via Halton Borough Council. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

<http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx>
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Data Protection Act 1998
http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

Email

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

Managing e-Mail

- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform (the ICT subject leader or headteacher) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the ICT National Curriculum.
- However you access your e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending Emails

- Use your own school e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

Check your e-mail regularly

- Never open attachments from an untrusted source
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is the headteacher. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance.

Senior Management and governors are updated by the Headteacher and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

The school provides opportunities within a range of curriculum areas to teach about eSafety

Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum

Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities

Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or

help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button

Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

eSafety Skills Development for Staff

Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages during staff meetings.

New staff receive information on the school's acceptable use policy as part of their induction

All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.

All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the headteacher or subject leader. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the subject leader or the school's computer support team. (HBC)

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the subject leader or Headteacher.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the subject leader or the headteacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the headteacher, depending on the seriousness of the offence; investigation by the Headteacher/ LA immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity

Staff will preview any recommended sites before use

Raw image searches are always supervised by staff.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

All users must observe copyright of materials from electronic resources

Internet Use

You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application

On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Managing Other Web Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the school endeavors to deny access to social networking (unless it is the school's Twitter page)

All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are

Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals

Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online

Our pupils are asked to report any incidents of Cyberbullying to the school

Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).

St Mary's CE Primary ensure that children are safe from terrorist and extremist material when accessing the internet in school. As with other online risks of harm, every teacher is aware of the risks posed by the online activity of extremist and terrorist groups. All staff undergoes Prevent training. Halton Borough Council provides St Mary's with web filtering to keep our children safe.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

Ensure that any school information accessed from your own PC or removable media equipment is kept secure

Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access

Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others

Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment

Only download personal data from systems if expressly authorised to do so by your manager

You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience

Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

Safe Use of Images and work

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images and use of pupil's work, by staff and pupils with school equipment

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

As a user of the school ICT equipment, you are responsible for your activity

It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

Ensure that all ICT equipment that you use is kept physically secure

Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

It is imperative that you save your data on a frequent basis to the school's share drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network

It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or

classified information is disclosed to any unauthorised person

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

All activities carried out on school systems and hardware will be monitored in accordance with the general policy

Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

The installation of any applications or software packages must be authorised by the Headteacher, fully licensed and only carried out by your ICT support

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use.

Pupils are allowed to bring personal mobile devices/phones if agreed with the Headteacher. This is at their own risk.

The school is not responsible for the loss, damage or theft of any personal mobile device

SUPPORTING DOCUMENTS

This policy, is linked to the following school policies:

- Keeping Children Safe in Education; Statutory guidance for schools and colleges (2016)
- Working Together to Safeguard Children (2015)
- Prevent Duty Guidance (HM Government 2015)
- Prevent Strategy (HM Government 2011)
- What to do if you're worried a child is being abused (2015)
- Information Sharing (DfE: 2015)
- Safeguarding and Child Protection Policy

- Health and Safety Policy
- Home School Agreement
- Behaviour Policy
- Anti-bullying Policy
- PSHCE Policy
- Staff Code of Conduct
- Freedom of Information Policy