ICT / e-Safety Policy

E-Safety Coordinator: Mark Bainton (Director of ICT)

Introduction

St Mary's recognises that the internet and other digital technologies provide a vast opportunity for pupils to learn. It allows for those involved in the education of the pupils to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement
- Develop the curriculum and make learning exciting and purposeful
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.

It is the duty of St Mary's School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of School include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video and audio conferencing;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use Agreement (for all staff, governors, volunteers, pupils, parents and visitors), is implemented to protect the interests and safety of the whole School community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following School policies:

- Safeguarding
- Behaviour
- Anti-Bullying
- Social Media
- Data Protection - Staff
- PSHE scheme of work
- Taking, Storing and Using of Images
- Privacy Notice

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

Scope of this Policy

This policy applies to all members of the School community, including staff, governors, volunteers, pupils, parents and visitors, who have access to and are users of the School ICT systems. In this policy 'staff' includes teaching and non-teaching staff, governors and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

Both this policy and the Acceptable Use Agreement cover both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto School premises (tablets, smart phones, etc.).

A. Roles and responsibilities

1. The Governing Body

The Governing Body of the School is responsible for the approval of this policy and for reviewing its effectiveness. It will review this policy at least annually.

2. Principal and the Senior Leadership Team

The Principal is responsible for the safety of the members of the School community and this includes responsibility for e-Safety. The Principal has delegated day-to-day responsibility to the e-Safety Coordinator.

In particular, the role of the Principal and the Senior Leadership team is to ensure that:

· staff are adequately trained about e-Safety; and

· staff are aware of the School procedures and policies that should be followed in the event of the abuse or suspected breach of e-Safety in connection to the School.

3. E-Safety Coordinator

The School's e-Safety Coordinator is responsible to the Principal for the day to day issues relating to e-Safety. The e-Safety Coordinator has responsibility for ensuring this policy is upheld by all members of the School community, and works with ICT staff to achieve this. They will keep up to date on current e-Safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

The Senior Leadership Team are updated by the e-Safety Coordinator at termly meetings and all Governors have an understanding of the procedures and strategies at our School in relation to e-Safety and local and national guidelines and advice. ICT and any e-Safety issues are also discussed and minuted at the Senior Leadership Team meetings.

4. ICT staff

The School's ICT staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School's hardware system, its data and for advising all staff regarding the use of ICT. They monitor the use of the internet and emails maintain content filters, and will report inappropriate usage to the e-Safety Coordinator.

5. All staff

All staff are required to sign the Acceptable Use Agreement; new staff do so as part of their induction.

As with all issues of safety at this School, staff are encouraged to create a talking and listening culture in order to address any e-Safety issues which may arise in classrooms on a daily basis.

6. Pupils

Pupils are responsible for using the School ICT systems in accordance with the Acceptable Use Agreement and for letting staff know if they see the ICT system being misused.

7. Parents and carers

St Mary's believes that it is essential for parents to be fully involved with promoting e-Safety both in and outside of School. We regularly consult and discuss e-Safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School. Parents and carers are responsible for endorsing the School's Acceptable Use Agreement for Pupils.

8. Visitors including Visiting Speakers

Visitors including visiting speakers will be accompanied by the staff organiser at all times.

B. Education and training

1. Staff: awareness and training

New staff receive information on St Mary's ICT / e-Safety Policy and Acceptable Use Agreement as part of their induction.

All staff receive regular information and training on e-Safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School e-Safety procedures. These behaviours are summarised in the Acceptable Use Agreement. When children use School computers, staff should make sure pupils are fully aware of and understand the agreement they have made by following the School's ICT guidelines.

Teaching staff are encouraged to incorporate e-Safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-Safety occurs and be provided directly to the School's Designated Safeguarding Lead.

2. Pupils: e-Safety in the curriculum

ICT and online resources are used increasingly across the curriculum. The School believes it is essential for e-Safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-Safety and regularly monitor and assess our pupils' understanding of it.

The School provides opportunities to teach about e-Safety within a range of curriculum areas, Computer Science and age-appropriate PSHE lessons. These include:

- General E-safety advice
- Social media / security settings
- Reporting issues
- Placing images online
- Legislation / data protection
- Disclosure of personal information
- Online fraud

Pupils are taught about their e-Safety responsibilities and to look after their own online safety. They are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across.

Pupils are aware of the impact of Cyberbullying and understand it will not be tolerated. Pupils know how to seek help if they are affected by any form of online bullying. They 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 Childline, NSPCC or CEOP report abuse button.

3. Parents

The School seeks to work closely with parents and guardians in promoting a culture of e-Safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

The School recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The School therefore arranges sessions for parents in order to offer advice about e-Safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

C. Use of personal devices (BYOD)

The School allows staff to bring in personal mobile phones and devices for their own use. Under normal circumstances, the School does not allow a member of staff to contact a pupil or parent/carer using their personal email or mobile phone number unless it is approved first by the Principal.

Pupils are allowed to bring personal mobile devices/phones to School but must not use them for personal purposes at any time. At all times the device must be switched onto silent.

Pupils' personal devices (tablets not phones) may be used for educational purposes, as agreed with the Teacher, during lesson time only.

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

The sending of inappropriate messages between any members of the School community is not allowed.

Permission must be sought from the Principal before any image or sound recordings are made on these devices by a member of staff.

No images, sound or video are to be used outside of the School environment.

No images, sound or video are to be uploaded to any social media sites.

Users bringing personal devices into School must ensure there is no inappropriate or illegal content on the device.

Privately owned ICT equipment can be linked to the wireless network but must not be connected to the main School network.

In the Early Years Foundation Stage (EYFS), staff must **not** in any circumstances use their

mobile phones to take photographs of the children. School hand-held devices must be used at all times and not be taken off site.

D. Use of School devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the School device which is allocated to them for School work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Staff are responsible for any activity undertaken on the School's ICT equipment provided to them.

Social Media (see also the Social Media Policy for Staff)

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with School work or business from School devices or whilst in front of pupils. Occasional access may only be made whilst in staff-only areas of School.

Staff must immediately report to the Senior Leadership Team the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the ICT Manager.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual; or
  - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should staff add pupils as social network 'friends' or contact them through social media.

Staff should:

- Not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data.
- Save their data on a frequent basis to the School's network drive. They are responsible for the backup and restoration of any of their data that is not held on the School's network drive.

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- Staff are able to download free Apps onto their school hand held devices.
- Paid APPs can only be downloaded by the network manager
- Staff should not attempt to download or install any software onto their school standalone machines. These must be authorised by the SLT, Director of ICT and installed by the network manager

Pupils

Pupils in years 3-11 are issued with their own personal School email addresses for use on the School network. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all School work e.g. assignments / research / projects. Pupils should be aware that email communications through the School network and School email addresses are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails (with attachments) and certain websites are automatically blocked by the School's filtering system. If this causes problems for School work purposes, pupils should make their teacher aware, who will in turn contact the ICT Manager for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to their teacher.

The School expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the class teacher who will complete the e-Safety Incident Report Form and pass it to the Designated Safeguarding Lead. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded and will be dealt with under the School's Safeguarding Policy. Pupils should be aware that all internet usage via the School's systems and its Wi-Fi network is monitored.

E. E-mail

The use of e-mail within School 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.

The School has taken all reasonable steps to ensure that the School network is safe and secure. The whole School community should be aware that email communications through the School network are monitored.

Managing e-mail: Staff

- The School gives all staff their own e-mail account to use for all School business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the 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.
- Staff must avoid contact with pupils, parents or conduct any School business using personal home 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.
- All e-mails between staff and pupils or parents / carers must be professional in tone and content.
- Teaching staff sending e-mails to external organisations, parents or pupils are advised to cc. the Principal, HOD or Line Manager.
- E-mails created or received as part of staff School activities could be subject to disclosure in response to a Subject Access Request under Data Protection Law. Staff must therefore actively manage their e-mail account as follows:
    - Delete all e-mails of short-term value.
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.
- Staff must inform the Senior Leadership Team if they receive an offensive e-mail.
- Staff access to their School e-mail (whether directly through webmail when away from the School or on non-School hardware) will be subject to this policy.

Managing e-email: Pupils

Pupils may only use School approved accounts on the School system for educational purposes.

Sending e-mail: Staff

- Staff must use their own School e-mail account so that they are clearly identified as the author.

  Staff should:
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Not send or forward attachments unnecessarily. Whenever possible, save the attachment to the shared drive rather than sending

Receiving e-mail: Staff

Staff should:

- Check their e-mail regularly.
- Activate their 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; consult the ICT Manager first.
- 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.

F. Internet Access

The internet is an open communication medium, available to all, 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: Staff

- Staff should preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that should have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.
- It is illegal to copy or distribute School software or illegal software from other sources.

Internet Use: Staff

It is at the Principal's discretion on what internet activities are permissible for staff and how this is disseminated.

- Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Staff must not reveal names of colleagues, customers or clients or any other confidential information acquired through their job on any social networking site or blog.
- Staff are aware that School based email and internet activity can be monitored and explored further if required.
- The School uses management control tools for controlling and monitoring workstations.
- If staff discover an unsuitable site, the website must be closed and the incident reported immediately to the Designated Safeguarding Lead.
- It is the responsibility of the School, by delegation to the ICT Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all School machines.
- Staff are not permitted to download programs or files on School based equipment.
- If there are any issues related to viruses or anti-virus software, the ICT Manager should be informed.

Internet Use: Pupils

Pupils are:

- Advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, School details, IM/ email address, specific hobbies/ interests)
- Advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Encouraged to be wary about publishing specific and detailed private thoughts

online.
- Asked to report any incidents of cyberbullying to the School.
- Aware that School based email and internet activity can be monitored and explored further if required.
- Pupils are not permitted to download programs or files on School based equipment.
- If pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and recorded on the e-Safety Incident Form.

G. Data storage and processing

Staff and pupils are expected to save all data relating to their work to their School laptop/ PC or to the School's central server.

Staff devices should be password / PIN protected if any data or passwords are stored on them.

No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by School.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Director of ICT.

H. Password security

Staff
Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff are aware of their individual responsibilities to protect the security and confidentiality of School networks, including the Management Information System.

All staff:
- must read and sign an Acceptable Use Agreement to demonstrate that they have understood the School's ICT/e-Safety Policy.
- are provided with an individual network, email and Management Information System log-in username.
- must enter their personal passwords each time they logon. Do not include passwords in any automated logon procedures.
- must change passwords whenever there is any indication of possible system or password compromise
- must not record passwords or encryption keys on paper or in an unprotected file.
- should ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

User ID and passwords for staff and pupils who have left the School are removed from the system as soon as is practicable.

I. Remote Access
Staff should treat the remote work place as if they are at work andare responsible for all

activity when using a remote access facility. Remote access includes Virtual Private Networks (VPNs) such as Splashtop and online facilities such as Office 365 and Microsoft Teams. The equipment must be running an up-to-date operating system, which is updated as and when appropriate. Staff must only use equipment with an appropriate level of security for remote access; this includes appropriate anti-virus software.

To prevent unauthorised access to School systems, staff must keep all access information such as logon IDs confidential and must not disclose them to anyon e.

Staff must avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify it.

School information and data must be protected at all times, including any printed material produced while using the remote access facility. Particular care must be taken when access is from a non-School environment. In the event that School data is lost, staff must report it immediately to the Senior Leadership Team and Data Protection Manager (the latter role is carried out by the Bursar). They will then discuss it and take advice, so that appropriate action can be taken.

J. Safe use of digital and video images (see also Taking, Storing and Using Images Policy)

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their children at School events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Agreement concerning the sharing, distribution and publication of those images. Those images must only be taken on School equipment: personal equipment must not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

Pupils must not take, use, share, publish or distribute images of others.

Written permission from parents or carers will be obtained before images of pupils are published on the School website.

Images published on the School website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

K. Video and Audio Conferencing

There will be occasions within school where pupils and staff are given the opportunity to engage in video or audio conferencing. This could be through Microsoft Office online tools, TEAMs (which is a secure video service) or through Zoom.

These activities are planned carefully to ensure they are age appropriate and clear guidelines have been shared to protect both pupils and staff. These are in-line with schools Acceptable Use Agreements and Safeguarding Policy.

If any video, audio conferencing is to be recorded, everyone involved must be made aware. A register of who is in attendance should be taken.

If any sharing of personal data is needed i.e. usernames to invite pupils/staff to join the group these will only be through school provided emails.

The Principal's approval is sought prior to any video or audio conferencing taking place be it within the school setting or when working remotely.

L. Misuse

St Mary's will not tolerate illegal activities or activities that are inappropriate in a School context, and will report illegal activity to the police and/or the Local Authority Designated Officer (LADO). Incidents of misuse or suspected misuse will be dealt with in accordance with the School's Safeguarding Policy.

The School will impose a range of sanctions on any pupil who misuses technology to cyberbully, harass or abuse another pupil in line with our Anti-Bullying Policy.

M. E-Safety incidents

Incidents of or concerns around e-Safety will be recorded using the e-Safety Incident Form and handed to the Designated Safeguarding Lead.

N. Complaints

As with all issues of safety at St Mary's, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-Safety, prompt action will be taken to deal with it.

Complaints should be addressed to the Principal, who will liaise with the e-Safety Coordinator and undertake an investigation where appropriate. The School's Complaints Procedure is available on our website.

Reviewed/Approved: Nov 2020
Next review: Autumn 2021

Incident Report Form – (including e-Safety and Bullying)

All incidents should be reported to the Designated Safeguarding Lead.

Date: _____

Name of person reporting incident: _____

Pupil(s) involved: _____

Location of incident

- ☐ In school (please specify)_____
- ☐ Outside of school (please specify)_____

Type of concern:

- ☐ Cyber bullying/harassment
- ☐ Bullying
- ☐ Deliberately bypassing security
- ☐ Accessing unsuitable content
- ☐ Racist, sexist or homophobic material
- ☐ Radicalisation or extremism
- ☐ Material of a sexual nature
- ☐ Other (please specify) _____

Nature of incident:

Deliberate access:

The material was:

☐ created ☐ viewed ☐ printed ☐ shown to others

☐ transmitted to others ☐ distributed

Accidental access:

The material was:

☐ created ☐ viewed ☐ printed ☐ shown to others

☐ transmitted to others ☐ distributed

Description of incident:

_____

_____

_____

_____

_____

_____
_____
_____

_____
_____
_____
_____

_____
_____
_____
_____

Action taken:

☐ Discussion with child ☐ Reported to Principal ☐ Parents informed

☐ Safeguarding referral ☐ Police informed

Details of Action Taken: