



St Mary's Church of England V.A. Primary School

e-Safety Policy



Introduction and Policy Aim

The purpose of this policy is to establish the ground rules we have in school for using I.T. equipment and the Internet.

An expanded document, "E-Safety Guidance", has been produced for the E-Safety Co-ordinator and Governor, and the ICT Co-ordinator and Governor to refer to for further information.

Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- access to illegal, harmful or inappropriate images or other content;
- unauthorised access to, loss of or sharing of personal information;
- the risk of being subject to grooming by those with whom they make contact on the Internet;
- the sharing/distribution of personal images without an individual's consent or knowledge;
- inappropriate communication/contact with others, including strangers;
- cyber-bullying;
- access to unsuitable video/Internet games;
- an inability to evaluate the quality, accuracy and relevance of information on the Internet;
- plagiarism and copyright infringement;
- illegal downloading of music or video files;

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

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour, Child Protection, Health & Safety and Safeguarding.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy that follows explains how St Mary's intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the ICT and E-Safety Coordinators;
- regular monitoring of e-safety incident logs;
- regular monitoring of filtering/change control logs; and
- reporting to relevant Governors and/or committee(s) meetings.

Headteacher & Senior Leadership Team (SLT)

- The Headteacher is responsible for ensuring:
 - the safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the E-Safety Coordinator;
 - adequate training is provided;
 - effective monitoring systems are set up; and
 - that relevant procedures in the event of an e-safety allegation are known and understood.

E-Safety Coordinator

The E-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in:

- establishing and reviewing the school e-safety policies and documents;
 - liaising with staff, the LA, ICT Technical staff, E-Safety Governor and SLT on all issues related to E-safety;
-

- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- providing training and advice for staff;
- receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;

ICT Coordinator

The ICT Coordinator is responsible for ensuring that:

- the school's ICT infrastructure is secure and meets e-safety technical requirements, ;
- the school's password policy is adhered to;
- SWGfL is informed of issues relating to its standard applied filtering policies;
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- he/she keeps up to date with e-safety technical information; and
- the use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator and Headteacher for investigation/action/sanction.

Note, currently St Mary's engages the services of the Gloucestershire County Council ICT Support Team for day-to-day support of the school's PCs, laptops, printers and servers. The ICT Coordinator therefore has an additional responsibility to ensure that the County ICT Support team adhere to the above e-safety measures during the course of their activities and are aware of the SWGfL Security Policy and Acceptable Usage Policy.

Teaching & Support Staff

In addition to elements covered in the Staff Accessible Usage Policy (AUP):

All teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the school Staff Acceptable Usage Policy (AUP);
- e-safety issues are embedded in all aspects of the curriculum and other school activities;
- pupils understand and follow the school's e-safety and acceptable usage policies;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extracurricular and extended school activities; and
- in lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Child Protection Officer

The school's Designated Child Protection Officers (DCPO) should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

Pupils (to an age appropriate level)

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so; and
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Usage Policy; and
- accessing the school website in accordance with the relevant school Acceptable Usage Policy.

Visitors

Visitors to St Mary's (eg supply teachers/work experience) who require access to the school's ICT systems will be expected to sign a Visitors Acceptable Usage Policy before being provided with such access.

Education and Training

E-safety education will be provided in the following ways:

- a planned e-safety programme is provided as part of ICT/PHSE/other lessons and is regularly revisited – this programme covers both the use of ICT and new technologies in school and outside of school;
- pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information;
- pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school;
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- rules for the use of ICT systems and the Internet are posted in school; and
- staff act as good role models in their use of ICT, the Internet and mobile devices.

Acceptable Usage Policy

- **parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules; and
- **staff and visitors** to the school have an AUP that they must read through and sign to indicate understanding of the rules.

Copyright

- pupils to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this;
- pupils are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- if using a search engine for images – staff / children should open the selected image and go to it's website to check for copyright; and
- the school endeavours to follow copyright legislation. It has put a disclaimer on website re copyright.

Training

- E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
 - a planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly;
 - all new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Usage Policies;
-

- the **E-Safety Coordinator** will receive regular updates through SWGfL, Local Authority and/or other information/training sessions and by reviewing guidance documents released by BECTA, SWGfL, the Local Authority and others;
- **governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Communication

Email

- **staff:** digital communications with pupils (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems;
- in the school context, e-mail should not be considered private;
- the school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems);
- the following disclaimer message should be attached to all e-mail correspondence:

This e-mail is only for the intended recipient. Its contents are subject to a duty of confidence and may be privileged. If you believe you have received this message in error, please advise the sender by reply immediately.

The views expressed in this message are not necessarily those of St Mary's Church of England Primary School or of Gloucestershire County Council.

- under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses;
- school e-mail is not to be used for personal use; and
- staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents / pupils.
- **pupils:** Should only use the school email system in school – under the supervision of a member of staff.

Mobile Phones

- all **school** mobile phones are barred from calling premium rate numbers and any numbers outside of the UK by default;
- **staff** should not be using personal mobile phones in school during working hours when in contact with children; and
- **children** are not allowed mobile phones in school.

Social Networking Sites (Children will not be allowed on Social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites).

- **staff:** Not to be accessed on school equipment in school or at home;
 - **staff** users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog;
-

- **staff:** Only to be accessed on non school equipment away from school;
- **pupils** in KS2 curriculum will be taught about e-safety on social networking sites as we accept some may use it outside of school; and
- if inappropriate comments are placed on Social Networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.

Digital Images

- **staff:** The school record of parental permissions granted / not granted must be adhered to when taking images of our children. This is based on the following three categories (central list kept in the office).
 - *I do/do not give permission for any image/photograph or video to be taken of my child whilst at school, for use in school.
 - *I do/do not give permission for any image/photograph or video to be taken of my child whilst at school, for use in local publicity in and around Tetbury, or in the local press.
 - *I do/do not give permission for any image/photograph or video to be taken of my child whilst at school for use in the public domain (i.e. on websites);
 - under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher or the ICT co-ordinator;
 - where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity;
 - children should not have full names by them in photographs - first name only; and
 - permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.
-

Removable Data Storage Devices eg memory sticks

- **staff:** Only school provided removable media should be used;
- all files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks; and
- **children:** Should not bring their own removable data storage devices into school unless asked to do so by a member of staff.

Websites

- **staff:** In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches;
- will preview any recommended sites before use;
- “open” searches (e.g. “find images/ information on...”)are discouraged when working with pupils;
- if Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research;
- **all** users must observe copyright of materials published on the Internet;
- **pupils** are not allowed unsupervised Internet access at any time in school. Teachers will carry out a risk assessment re which children are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the children on the internet by the member of staff setting the task. All staff are aware that if they pass children working on the internet that they have a role in checking what is being viewed; and
- the school only allows the E-Safety Co-ordinator, ICT co-ordinator and Headteacher access to Internet logs.

Passwords

- **staff:** Passwords or encryption keys should not be recorded on paper or in an unprotected file;
- passwords should be changed annually – at the start of September;
- users should not use the same password on multiple systems or attempt to “synchronise” passwords across systems; and
- **children:** should only let the school staff know their in-school passwords.

Monitoring


- all use of the school's Internet access is logged and the logs are randomly but regularly monitored by SWGfL. Whenever any inappropriate use is detected it will be followed up by the E-Safety Co-ordinator;
 - E-Safety Coordinator and, if not the same person, the Headteacher will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems;
 - no additional monitoring systems are currently deployed at St Mary's; and
 - any technician or member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the E-safety co-ordinator and impounds the equipment. This is part of the protocol / job description for Technicians. (If the concern involves the E-Safety co-ordinator then the member of staff or technician should report the issue to the E-Safety Governor).
- **Incident Reporting**

Any e-safety incidents must immediately be reported to the Headteacher or E-Safety Coordinator who will follow the guidance in the "E-Safety Guidance" document.

Use of Own Equipment

- **staff:** No school business should be conducted on privately owned equipment;
- privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher or ICT co-ordinator; and
- **children** should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- **all:** No personally owned applications or software packages should be installed on to school ICT equipment;
- **staff:** Personal or sensitive data should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted; and
- ensuring any screens are locked (by pressing +L) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

AUPs to be added
Acronyms

Consultation: February 2011

Policy Review

This e-Safety Policy shall be reviewed annually by the Curriculum Committee, with any recommended changes approved by the full Governing Body.

The next review is due on, or prior to, 1st December 2012.

Signed:

Date: 6th December 2012
