



St Mary's and St Peter's CE Primary School

eSafety

| | | | |
|--------------|------------|---------------------|----------------|
| Date: | April 2018 | Review Date: | September 2018 |
|--------------|------------|---------------------|----------------|

Our school is a Church of England School and works in partnership with our two local parish churches, St Mary with St Albans and St Peter and St Paul's. We aim to reflect the values, traditions and beliefs of the Christian Faith and therefore our Spiritual Values underpin everything that we do.

We believe high standards of care and love are an integral part in the quality of teaching and learning across the whole curriculum. Our school Christian vision of 'Life in all its fullness' applies to all areas of our school. The two great commandments given by Jesus will underwrite the life of our school; they are to 'love God' and to 'love your neighbour as yourself'. It is our aim for both of these instructions to be evident in the whole life of the school, in the relationships between all members of the community, pupils, staff and parents.

St Mary's and St Peter's school fully recognises its moral and statutory responsibility to safeguard and promote the welfare of pupils. Our KS2 eSafety Policy is one of a range of documents which set out the safeguarding responsibilities of the school. We wish to create a safe, welcoming and vigilant environment for children where they feel valued and are respected.

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

Aims

- To outline the schools provision for eSafety teaching to the school community.
- To outline the technical and behavioural structures in place to protect the school community.

Internet Access

- At Key Stage 1, access to the internet is via a class log-in and should only take place under direct supervision using vetted on-line materials.



St Mary's and St Peter's CE Primary School

- At Key Stage 2, only pupils who have signed the Acceptable Use Policy will be permitted personal access via an individual log-in. Internet use should only take place with permission from a present member of staff.
- Parents will be asked to sign and return the AUP along with their children to confirm their consent.
- Personal e-mail accounts may be provided to individual KS2 users, but will be limited to internal and approved communications only.
- Staff access to the Internet is subject to a more comprehensive Acceptable Use Agreement.

Infrastructure

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the following sections will be effective in carrying out their eSafety responsibilities:

- School ICT systems are managed in ways that ensures the school meets the eSafety technical requirements outlined in the Data Security Policy and Acceptable Usage Policy and any relevant Local Authority eSafety Policy and guidance;
- There are regular reviews and audits of the safety and security of school ICT systems;
- Servers, wireless systems and cabling are securely located and physical access restricted;
- All users have clearly defined access rights to school ICT systems.
- The “master / administrator” passwords for the school ICT system, are kept secure and only know to the School Technician, eLearning coordinator and approved external technical services;
- Individual users are responsible for the security of their username and password and must not allow others unsupervised access the systems using their log on details. Any suspicions or evidence of a misuse of access credentials must be immediately reported to the eLearning coordinator, on-site technical or the headteacher;
- The school’s Internet service is filtered by the LGfL service, in accordance with their policies, which the school abide by;
- Overriding of the LGfL filtering settings can only be performed under approval from the eLearning co-ordinator or a member of senior management after due consideration of the risks & benefits.
- The eLearning coordinator and on-site technician regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users’ activity;
- Appropriate security measures are in place (in the form of access keys, encryption, passwords and physical security) to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.



St Mary's and St Peter's CE Primary School

- Established logins are provided for limited, temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy is in place (see Acceptable Use Policy & Data Security Policy) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place (see Acceptable Use Policy) that details staff permissions to install programmes on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data is not permitted to be sent over the internet or taken off site unless safely encrypted or otherwise secured (see Data Security Policy).
- The school employs a sophisticated monitoring system to record and notify the eSafety Officer of any breaches in this policy, including potential Child Protection issues. All users of the school ICT system are subject to this monitoring and are made aware through the Acceptable Use Policy.

eSafety Curriculum

Students

eSafety education for students will be provided in the following ways:

- A planned eSafety programme will be provided as part of Computing and PHSE lessons. The themes of these lessons are tailored to the age-range, technological experiences and practical applications of the individual year groups;
- Key eSafety messages are reinforced as part of a planned programme of assemblies;
- Pupils are helped to understand the need for the Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices (where appropriate) both within and outside school;
- Rules for the appropriate and safe use of ICT systems are presented to children every time they access the network;
- Staff are expected to act as good role models in their use of ICT, the internet and mobile devices.

Parents

The school will seek to provide information and awareness to parents and carers through:

- Letters, newsletters, pamphlets and the school website;
- Internet Safety talks;
- Reference to relevant eSafety websites

Staff

All staff members should ensure their own understanding of eSafety issues is kept up to date through:

- Training sessions;
- Reference to relevant eSafety websites;
- eSafety bulletin updates;
- Informal updates from the eLearning coordinator or School Technician;

Use of ICT in school



St Mary's and St Peter's CE Primary School

eSafety should be a focus in all areas of the curriculum and staff are expected to reinforce eSafety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet (e.g. using search engines), staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of Digital Image and Work

The school will inform and educate users about the risks associated with posting material online and will implement policies to reduce the likelihood of the potential for harm:

- During eSafety sessions, pupils will be educated about the issues of consent and 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, eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images (see Data Security Policy & Acceptable Use Agreement).
- Care should be taken when taking digital / video images that students / 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 without their consent.
- Under the terms of the Data Protection Act 1998, parents, friends and family members can take images of their children and friends participating in school activities for family and personal use.
- If the recording is not for personal use e.g. with a view to selling the video, then consent of other parents whose children may be on film would be required. Without this consent, the Data Protection Act would be breached.
- Parents are allowed to film school events such as sports days, fetes and school plays so long as the performance is not disturbed.

Online Publishing

- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be published anywhere on any school website, video or digital attachment - particularly in association with photographs.



St Mary's and St Peter's CE Primary School

- Parents will be regularly informed of their right to not have their child's image on the school website and that if they do not notify the school, consent will be assumed. Where barriers may prevent informed consent (e.g. parents with little/no English), written consent will be sought.
- Pupil's work can only be published with the permission of the pupil.
- Consent is not required where either individuals cannot be identified or they for part of a large crowd at a public event.
- Parental consent can be withdrawn or changed at any time in writing.
- Pupils should only publish material to approved, educationally-related websites.
- Pupils should only Publish material that is:
 - not copyrighted;
 - their own work (or with permission of the owner);
 - not offensive or embarrassing to another individual;
 - approved by a member of staff.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school will ensure compliance with this by following the Data Security Policy.

Online Activities

- **Newsgroups** will not be made available to pupils unless an educational requirement for their use has been demonstrated.
- Access to **forums** that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted.
- Pupils will not access **social networking sites** for example 'Facebook'.
- Children should use only regulated, educational **chat** environments. This use will be supervised and the importance of chat room safety emphasised.
- Pupils use of personal messaging services (for example, 'WhatsApp') is not permitted.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.
- Use of **video conferencing** systems should only take place under staff supervision.
- Students should not be permitted to **register** themselves on external sites without parental consent. Teachers may, however, create 'class' accounts where educational relevant without parental consent.



St Mary's and St Peter's CE Primary School

- The school may register pupils on external websites where the school has an active, approved subscription for educational purposes and the risks & benefits have been adequately considered.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure.
- Users need to be aware that email communications may be monitored by automated systems reporting to the eLearning coordinator.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents (email, text message, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications. The only exception to this rule would be if, while on a school trip, a staff member has pressing need to contact a parent using their own device.
- Whole class or group email addresses will be used at KS1, while students / pupils at KS2 and above may be provided with individual school email addresses for educational use.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

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.

Responding to Incidents

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or (very rarely) deliberate misuse.

Apparent or actual misuse that appears to involve illegal activity will be reported immediately to the police for further investigation. Examples of illegal misuse include:

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials.



St Mary's and St Peter's CE Primary School

Incidents of misuse will be dealt with as soon as possible and in a proportionate manner. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as outlined in the Acceptable Use Policy.

| | | | |
|---------------------------------|--|--------------|--|
| Headteacher: | | Date: | |
| Chair of Governing Body: | | Date: | |