St Anne's Catholic Primary School

E-Safety Policy

Policies and procedures are based on the use of 360° Safe tool (offline) and Ofsted Guidance.

'St. Anne's is committed to taking appropriate action with regard to e-safety incidents involving its pupils that occur outside the school through the involvement of staff generally and the Leadership Team specifically.'

Rationale

New technologies have become integral to the lives of children and young people in today's society, and for the 21st century, both within schools and in their lives outside school.

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.

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

Unfortunately, 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, video games or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact with on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers,
- Sexting
- Implications of Geolocation
- Cyber-bullying
- 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 "offline world" and it is essential that this e-safety policy is used in conjunction with other school policies (eg anti-bullying, child protection and data protection policies

Scope
This policy applies to all members of the school community including staff, pupils and visitors

Technical/infrastructure/equipment

- All users will have clearly defined access rights to school ICT systems.
- Users will be made responsible for the security of their username and password, and must not allow other users to access the systems using their log on details
- The school maintains and supports the filtering system as recommended by Coventry LA
- An appropriate system is in place (to be described) for users to report any actual / potential e-safety incident on the Network
- An agreed policy is in place regarding the downloading of executable files by users and the installation of software.
- Personal data about staff or pupils cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured
- USB devices may only be used on the Network after having been virus checked

Curriculum/Pupil Use

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision.
- A planned e-safety programme will be provided as part of computing / and PSHCE / other lessons and will be regularly revisited by the pupils to learn the risks of e-communication (personal details, viruses, phishing, cyber-bullying, Internet risks, copyright, longevity of posted information/images etc.)
- Key e-safety messages are reinforced in assemblies

- Rules for use of ICT systems / internet are posted in rooms
- Pupils may only use computers/digital resources under the supervision of a member of staff – the adult may not necessarily be standing over them and the pupils have responsibility for following the *Responsible Computer Use* rules at all times.
- KS2 pupils may only use the Internet to search for resources to use in school-work.
- The use of websites for other purposes i.e. to play games, is only permitted by prior agreement with a member of staff. Lunch Clubs may only access approved sites.
- Pupils must ask for permission before searching using Google Images.
- ***Pupils not using computers responsibly will be denied freedom of access****.*
- Pupils must be advised as to the social, health and emotional impact of the excessive use of e-technologies.
- The school has the right to confiscate electronic devices, and to search for and delete information from them, as per the school Behaviour Policy.

Images

- Pupils must attain the permission of the subjects of all digital images and agree the purpose of their use, before using them.
- Publication of video/still images is subject to the approval of the participants and where appropriate, parents/guardians.
- Images of pupils/use of names may not be published for access externally without the permission of the Headteacher/ Deputy Head, unless covered by the Digital Image Consent Form.
- When using digital images, staff should inform and educate students / 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 images on the internet eg on social networking sites.

Information

- Pupils may only take digital information from school (via USB or VLE) with the permission of a member of staff. The information should be focused on learning.
- During computing lessons, pupils will be made critically aware of plagiarism, quality, accuracy, bias and relevance of information. This work will be followed up when cross-curricular opportunities arise.

Communication

- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details and conversing with strangers. They should 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.

- Users must immediately report 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 / pupils or parents / carers (email, chat, VLE etc) must only take place on official (monitored) school systems.
- All incidents must be reported by the pupil to the class teacher, who can inform the Network Manager/ Headteacher if appropriate.

Monitoring and Review

- Incidents must be logged in the E-Safety log book (which can be found in the staff room) and communicated to the E-Safety Officer.
- Staff will be kept up to date with developments via staff meetings/training.

E-Safety - Roles and Responsibilities

Governors – are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher–responsible for ensuring the safety (including e-safety) of members of the school community.

E-Safety Officer - takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.

Pupils are responsible for using the school ICT systems in accordance with the *Responsible Computer Use* rules. *Responsible Computer Use* rules reviewed periodically by School Council.

Parents / Carers endorse (by signature) the Pupil Acceptable Use Policy + Digital Image Consent Form. Website signposts parents to advice and guidance regarding online safety

Network Manager is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- there will be regular reviews and audits of the safety and security of school ICT systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher

School Staff (teachers and support staff) are responsible (as relevant) 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 Computer Security Guide.
- e-safety issues are embedded in the curriculum and other school activities

- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- processes are in place for dealing with any unsuitable material that is found in internet searches.
- they monitor ICT activity in lessons, extra curricular and extended school activities such as use of the VLE.
- they are aware of e-safety issues related to the use of mobile phones, usb sticks, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- they report any suspected misuse or problem to the E-Safety Officer/ Network manager.
- digital communications with students / pupils (email / VLE / voice) should be on a professional level and only carried out using official school systems
- **Data** is stored securely, computers are logged off after use and data is not transferred externally without having a secure password or being encrypted. **(More detailed information on data protection can be found via the Torbay Intranet, policies on 'Insight', on the school website and in the policy file in the staffroom.)**
- Only legal copies of software are used with the consent of the Network Manager, after being virus checked.