



E-Safety Policy

Aims of the School

1. *The school aims to show concern, in a school that looks to Christ for the basis of its existence, for all the teaching staff together with all the non-teaching staff and parents, as well as the pupils.*
2. *The school aims, through prayer, worship and liturgy, to develop the Faith of each individual in the school community.*
3. *The school aims to ensure that the curriculum provides a Catholic Christian setting in which the children can grow in Faith and understanding and in the acquisition of skills, attitudes, values and knowledge.*
4. *The school aims to prepare the pupils to become active and responsible within the home, school, parish and the wider community in which they may live.*

MISSION STATEMENT

*At St. Anthony's we believe
we are a community striving
to live, love and learn together
joyfully following Jesus Christ.*



St Anthony's Catholic Primary School E-Safety Policy

Our e-Safety Policy has been written using the SMBC Schools e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors.

The e-Safety Policy and its implementation will be reviewed regularly.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

Internet use is part of the statutory curriculum and a necessary tool for learning. Internet access is an entitlement for students who show a responsible and mature approach to its use.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries and to experts in many fields for pupils and staff;
- inclusion in the National Education Network connecting all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;

- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with SMBC and DCFS;
- access to learning wherever and whenever convenient.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils

Rules for Internet access will be posted in all networked rooms.

Pupils will be informed that Internet use will be monitored.

An e-Safety training programme will be delivered to all pupils to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools this will focus on PSHE and ICT areas of learning.

Instruction in responsible and safe use should precede Internet access and should be reinforced at regular intervals.

A module on responsible Internet use will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

Staff

All staff will be given the School e-Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

Parents

Parents' attention will be drawn to the e-Safety in newsletters, the school prospectus and on the school Website.

Internet issues will be handled sensitively to inform parents without alarm.

A partnership approach with parents will be encouraged. This could include parents' meetings such as "Inspire" with demonstrations and suggestions for safe home Internet use.

Internet access

The school will maintain a current record of all staff and pupils who are granted Internet access.

At Key Stage 1, access to the Internet will be by directly supervised access to specific, approved on-line materials.

Older primary children (KS2) and all secondary students must agree to comply with the Responsible Internet Use statement before they are granted access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Solihull ICT Services, and where appropriate the headteacher.

Online Materials

The evaluation of on-line materials is a part of the ICT Schemes of work. The school's website can be accessed by anyone. Publication of information will be considered from a security viewpoint.

Images

Photographs on websites that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

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

Images of staff should not be published without consent.

Social Networking

Social networking sites can connect people with others for a wide range of purposes,

Social networking sites and newsgroups will be blocked unless a specific use is approved.

Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.

Teachers should not communicate with pupils through private social networking sites, even on educational matters, but should use official sites sanctioned by the school.

Incidents of bullying through social networking will be dealt with in line with the school policy on bullying.

Filtering

The school will work in partnership with Solihull MBC and Becta to ensure filtering systems are as effective as possible.

If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the head teacher.

Email

Pupils and staff may only use approved email accounts on the school system for school business.

Pupils must immediately tell a teacher if they receive offensive email.

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Management Information Systems

The security of the school information systems will be reviewed regularly.

Virus protection will be updated regularly.

This is done via the Solgrid System

Personal data sent over the Internet will be encrypted or otherwise secured.

Portable media may not be used without specific permission followed by a virus check. Where they are used to store personal information they will be encrypted

Data Protection

Personal data will be recorded, processed, transferred and made available in compliance with to the Data Protection Act 1998.

The eight principles are that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Held no longer than is necessary
6. Processed in line with individuals rights
7. Kept secure
8. Transferred only to other countries with suitable security measures.

Complaints

Formal complaints of Internet misuse will be dealt with by a senior member of staff

Any complaint about staff misuse must be referred to the head teacher who should use the agreed SMBC procedures.