St. Peter's Catholic School

e-Safety Policy

Our e-Safety Policy builds on the SMBC Schools' e-Safety Policy and government guidance.
The e-Safety Policy and its implementation will be reviewed annually; Governors, Parents and Staff will be consulted.

Roles and Responsibilities
Governors delegate to Headteacher/Deputy Headteacher.
The School e-Safety Co-ordinator is Mrs. M. Murphy, Headteacher and a Designated Safeguard Lead responsible for Child Protection.
The ICT Manager is responsible for the running of any technical aspects of school safeguarding systems.
The e-Safety committee is responsible for the continued training of the governors, staff and students and will offer e-Safety Parents' Evenings to educate parents.
All classroom-based staff are responsible for teaching safe and responsible usage in their subject areas and for reporting e-Safety issues through the appropriate channels in line with the school policy.

The School recognises why Internet use is important

- 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. The school will continue to educate the students on the safe use of the Internet outside of school as part of their safeguarding policy and will offer support to parents to ensure that they are aware of appropriate filters they can use to safeguard their children whilst using devices through their Internet Service Providers (ISP).

Safe Internet use to enhance learning

- The School Internet access will be designed expressly for pupil use and will include appropriate filtering 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 safe 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.

Safe and Responsible Use – Pupils

- Rules for Internet access are posted in all classrooms.
- Pupils will be informed that Internet use will be monitored through appropriate filtering software in school.
- An e-Safety training programme is delivered to all pupils during the start of Year 7 to raise awareness and the importance of safe and responsible use of the Internet and other electronic communications tools.

- Continual updates and training will be provided throughout the year to all year groups to reinforce and update current trends and appropriate use of Internet sites and technology on mobile devices as part of our safeguarding policy.

Safe and Responsible 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 through appropriate filtering software and traced to the individual user. Discretion and professional conduct is essential.
- Filtering and monitoring of the school network is performed by ICT Support and breaches of school policy are reported accordingly.
- Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required. Policy consultation, regular reminders from the e-Safety committee and through email/briefings/bulletin and individual advice from Deputy Headteacher/Headteacher.

Safe and Responsible Use – Parents

- Parents attention will be drawn to the School e-Safety Policy 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 includes Parents' Evenings held throughout the year with demonstrations encouraging suggestions for safe home Internet use and protection on mobile devices. This includes the apps downloaded to mobile devices and suggestions on updating privacy settings and appropriate filtering through their ISP.
- Advice to enhance the responsible use of the Internet will be made available to parents on request.

Internet Access

- All users must read, sign and abide by the "Acceptable ICT Use Policy" before using any school ICT resource.
- The school recognises that 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 Headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

Pupils Evaluating Internet Content

- The school 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 when using the school network, the URL (address), time, date and content must be reported to ICT Support and where appropriate the school e-Safety Officer.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- They will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Managing the School's Public Website

- Staff or pupils' personal information will not be published.
- The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- The ICT Manager is responsible for ensuring that the content meets the statutory requirements and is appropriate.

Publishing Images of Pupils

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- If a name is to be used with a photograph which identifies a student, for example in a press release, we will ask permission from parents.

Managing Social Networking (see also Social Media Policy)

- Social networking sites and newsgroups will be blocked unless a specific use is approved for a short period of time to enhance the teaching and learning.
- 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, e-mail address, names of friends, specific interests and clubs, pictures of them in their school uniform etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and ensure their privacy settings are enabled. Advice will be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name, school or shopping centre. These issues will be reinforced by continued updates by the e-Safety committee throughout the year.
- Teachers should not run social network spaces for students on a personal basis. Teachers should not communicate with pupils through private social networking sites, even on educational matters, but should use the official school email system.
- Pupils will be advised by the e-Safety committee and staff on security denying access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others. They should be advised not to publish specific and detailed private thoughts.
- The school is aware that bullying can take place through social networking Incidents of bullying through social networking may be dealt with by the e-Safety committee in line with the school policy on bullying.

Managing Filtering

- The ICT Manager will work in partnership with Solihull MBC 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 ICT Manager or a member of the e-Safety committee.
- The ICT Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing E-mail

- Pupils should only use the school provided email account when contacting staff.
- Pupils must immediately tell the ICT Manager, a member of the e-safety committee or report to a teacher (who will follow the guidelines on the e-safety policy) if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations should be written carefully and authorised before sending in the same way as a letter written on school headed paper.

Video Conferencing

  - Teachers or support staff should be present when pupils are making or answering a videoconference call. Teachers or support staff should stay for the duration of the conference call.
  - Video conferencing should be supervised appropriately for the pupils' age.

    - Responsibility for the use of the video conferencing equipment outside school time needs to be established with care.
- Content
    - Recorded material shall be stored securely.
    - If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).
    - Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Bring Your Own Device (BYOD) are permitted by **authorised users** who have been given permission by the Leadership Team.
- Mobile phones will not be used during lessons or form time or seen during the school day.
- Sixth Form students may check their phones ONLY in the common room area or Room 30 (they will be confiscated if this privilege is misused).
- Smart watches are not permitted in school.
- Risk Awareness: The School recognises the pace of change in communication and the necessity for on-going assessment of new and emerging risks. The e-safety committee will continue to assess emerging risks from new technologies and updates policies, raise awareness to teachers and support staff in line with its responsibilities on e-safety safeguarding.
- Staff are not permitted to use personal equipment to video or photograph students or staff. Teachers should book and use the available resources from the ICT team to capture pictures or record footage of activities which relate to their learning. Pictures or video footage should only be taken when relating to the teaching and learning of the class or individual. This material should only be downloaded to the secure school system and not stored on staff personal devices. Failure to store this in appropriate places may lead to disciplinary action.
- Staff will be issued with a school phone where contact with pupils is required. Staff are not permitted to use personal phones to contact students via calls or text messages.
- Staff are not permitted to accept students as friends on social networking sites such as Facebook or through social media apps such as Instagram.

Managing Information Services

- The security of the school information systems will be reviewed regularly.
- Network-Threat protection will be updated regularly.
- Security strategies will follow Solihull MBC guidelines.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Confidential information should not leave the school network and not be stored on personal devices.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The ICT Manager will review system capacity regularly.

Protecting Personal Data

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

E-Safety Complaints

- Formal complaints of Internet misuse will be dealt with by the Lead Tutor or Leadership Team who may consult the e-safety committee for guidance.

- Any complaint about staff misuse must be referred to the Headteacher who should use the agreed SMBC procedures.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the e-safety committee to resolve issues.
- Sanctions for pupils within the school discipline policy include:
    - Interview/counselling by Lead Tutor or Leadership Team.
    - Informing parents or carers.
    - Removal of Internet or computer access for a period.
    - More serious sanctions/exclusion if bullying or repeated misuse.
    - External agencies may become involved for serious actions such as sexting, trolling or promoting radicalisation.

Community Use of ICT and the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites and the e-safety committee will offer appropriate advice.

Mobile Phone Policy for Parents and Visitors

- All visitors to the school are handed a 'safeguarding pack' this includes our Mobile Phone Policy detailed below:

Mobile Phone Policy for Parents and Visitors

Use of Mobile Phones:

- We request that parents and visitors do not use mobile phones, or any other device capable of recording images, in the school building or grounds unless in an emergency.
- Mobile phones, or any other device capable of recording images, must never be used to take photographs in the school building or grounds unless permission is granted by the Senior Leadership Team.
- Visitors will be asked to switch off their mobile phones whilst on the school premises and refrain from using them.