ST. MARY'S CATHOLIC PRIMARY SCHOOL,
STUDLEY

E-Safety Policy

Headteacher O. Finnegan

Chair of Governors S. Coyne

St. Mary's Catholic Primary School, Studley

E-Safety Policy

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT and for child protection.

> *The school has appointed Mr Owen Finnegan as e-Safety coordinator and the Designated Child Protection Coordinator.*

The school was registered for the 360° E Safety mark and is committed to achieving 360° Accreditation.

Teaching and learning

Why Internet use is important

- *Internet use is part of the statutory curriculum and a necessary tool for learning.*
- *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.*

Internet use will enhance learning

- *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 given clear objectives for Internet use.*

Pupils will be taught how to evaluate Internet content

- *If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service, and where appropriate the school e-safety officer.*
- *School will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.*

Managing Internet Access

Information system security

- *The security of the school information systems will be reviewed regularly.*
- *Virus protection will be installed and updated regularly.*
- *The school uses the Warwickshire Broadband with its firewall and filters.*
- *The school provides an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Service.*

.

E-mail

- *Pupils may only use approved e-mail accounts on the school system.*
- *Pupils must immediately tell a teacher if they receive 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.*
- *Use of words included in the Policy Central 'banned' list will be detected and logged.*

Published content and the school web site

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

Publishing staff and pupil's images and work

- *Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.*
- *Pupils' full names will not be used anywhere on the Web site or on the school Twitter site, with photographs of the child.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site and or Twitter site. This is conducted annually.*

Social networking and personal publishing

- *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, e-mail address, names of friends, specific interests and clubs etc.*
  (The school has a separate policy relating to social networking – see safeguarding folder).

Managing filtering

- *The school will work in partnership with the Warwickshire ICT Development Service 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 school E-Safety coordinator.*

Managing videoconferencing

The equipment and network

- *All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.*
- *IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.*
- *Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.*
- *External IP addresses should not be made available to other sites.*

Users

- *Pupils should ask permission from the supervising teacher before making or answering a videoconference call.*
- *Videoconferencing should be supervised appropriately for the pupils' age.*

Content

- *When recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.*

- *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).*

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.*

Protecting personal data

- *Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.*
  (The school has a separate policy relating to data protection).

Policy Decisions

Authorising Internet access

- *The school will maintain a current record of all staff and pupils who are granted Internet access.*
- *All users must read and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource.*
- *At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.*

Assessing risks

- *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor WCC can accept liability for the material accessed, or any consequences of Internet access.*
- *The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.*

Handling e-safety complaints

- *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 WCC procedures.*
- *A record of any internet incident is kept by the headteacher.*

Communications Policy

Introducing the e-safety policy to pupils

- *Rules for Internet access will be posted in the ICT suite.*
- *Pupils will be informed that Internet use will be monitored.*
- *An annual e-safety week will be held to remind children (at an age appropriate level) as to the dangers associated with the internet and issues directly related to the school's internet policy.*
- *Regular school assemblies led by RP, ICT co-ordinator are held. They are scheduled and delivered termly and will reinforce safer on-line practice and current safety issues related to protection and safety of children.*

Staff and the e-Safety policy

- *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.*
- *All staff should read and sign the school's Acceptable ICT Use Policy.*

Enlisting parents' support

- *Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Website.*
- *The school's newsletter regularly features items concerning online safety and will signpost parents to various resources which can assist further.*
- *Internet issues will be handled sensitively to inform parents without alarm.*
- *A partnership approach with parents will be encouraged. This could include parents' evenings with demonstrations and suggestions for safe home Internet use.*
- *Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.*

APPENDIX A

SANCTIONS FOR MISUSE OF SCHOOL ICT

Individual schools are responsible for deciding what sanctions will be applied for breach of acceptable ICT use policies. Sanctions applied should reflect the seriousness of the breach and should take into account all other relevant factors.

1.0 Sanctions for pupils

1.1 Category A infringements

These are basically low-level breaches of acceptable use agreements such as:

- Use of non-educational sites during lessons
- Unauthorised use of email or mobile phones
- Unauthorised use of prohibited sites for instant messaging or social networking.

The class teacher will refer such misdemeanours to the e-safety designated officer who will discipline in line with the school's policy.

School policy

1.2 Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of e-safety policy that are non-deliberate, such as:

- continued use of non-educational sites during lessons
- continued unauthorised use of email or mobile phones
- continued use of prohibited sites for instant messaging or social networking
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions could include:

- referral to e-safety contact officer
- loss of internet access for a period of time
- contacting parents.

School policy

1.3 Category C infringements

These are deliberate actions that either negatively affect the school system or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- cyber bullying

- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

Sanctions could include:

- referral to e-safety contact officer
- referral to head teacher
- loss of access to the i-pads/internet
- contacting parents
- any sanction agreed under other school policies

1.4 Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- persistent and/or extreme cyber bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions could include:

- referral to head teacher
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer
- referral to Warwickshire's e-safety officer.

School policy

2.0 Sanctions for staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

2.1 Category A infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the head teacher.

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (eg: removable memory sticks) without carrying out virus checks

- any behaviour on the world wide web that compromises the staff member’s professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user’s passwords
- breaching copyright or licence by installing unlicensed software.

Possible sanctions include referral to the head teacher who will issue a warning.

School policy

2.2 Category B infringements

These infringements involve deliberate actions that undermine safety of the school system and activities that call into question the person’s suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Safeguarding and Social Care. These include activities such as:

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Possible sanctions include:

- referral to the head teacher
- removal of equipment
- referral to Warwickshire’s e-safety officer
- referral to SSC or police
- suspension pending investigation
- disciplinary action in line with school policies