# ALL SAINTS' CofE JUNIOR SCHOOL & EMSCOTE INANT SCHOOL

# E-SAFETY POLICY

**Background**

E-safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The schools' e-safety policy should operate in conjunction with other policies including those for behaviour, anti-bullying, curriculum, data protection and security.

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Warwickshire Broadband including the effective management of Websense filtering and Policy Centre monitoring.
- National Education Network standards and specifications.

## 1.1 Writing and Reviewing the E-safety Policy

The e-safety policy is part of the schools' development plan and relates to other policies including those for ICT and for child protection.

- The e-safety governor is **Margherita Finney** – she also has responsibilities as a designated child protection co-ordinator. The e-safety committee is made up of pupils/governor/SLT/teacher and teaching assistant.
- The e-safety policy has been written by the school, building on the Warwickshire ICT Development Service e-safety policy and government guidance. It has been agreed by the senior management and approved by governors.
- The e-safety policy will be reviewed annually.

## 1.2 Teaching and Learning

1.2.1 Why Internet use is important

- The internet is an essential element in 21st century life for education, business and social interaction. The schools have a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2.2 Internet use will enhance learning

- The schools' 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.
- 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' ages and maturity and educate them in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.3 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 schools' e-safety officers.
- Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be crucially aware of the materials they read and shown how to validate information before accepting its accuracy.

**1.3 Managing Internet Access**

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The schools use the Warwickshire Broadband with its firewall and filters.
- The schools provide an additional level of protection through their deployment of Policy Centre in partnership with Warwickshire ICT Development Service.

1.3.2 Email

The ICT Development Service recommends that pupils and staff use the individual We-Learn email accounts provided through the Warwickshire Learning Platform for all school communications.

Staff and students need to understand that the use of the schools' network is a privilege which can be removed should reason arise. The schools may monitor all network and internet use in order to ensure student safety. All users should be expected to adhere to the generally accepted rules of network etiquette (netiquette). These include but are not limited to the following:

- Be Polite
- Use appropriate language
- Do not get abusive in your messages to others.
- Do not reveal the personal address, phone number or other personal details of yourself or other users.
- Do not use the network in such a way that would disrupt the use of the network by other users.
- Illegal activities are strictly forbidden.
- Note that email is not guaranteed to be private.
- System administrators have access to all mail.
- Messages relating to or in support of illegal activities may be reported to the authorities.

1.3.3 Published content and the schools' web sites

- The contact details on the web site should be the school address, email and telephone number. Staff or pupils personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing pupils' images and work

- Photographs 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 web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.
- Pupils' work can only be published with the permission of the pupil and parents.

1.3.5 Social networking and personal publishing

- Social networking 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.
- Pupils and parents will be advised that the use of social networking spaces outside of school may be inappropriate for primary-aged pupils.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location, such as house number, street name, school or shopping centre.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for students on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny 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.
- Students should be advised not to publish specific and detailed private thoughts.
- School staff and parents should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

1.3.6 Managing filtering

- The schools currently uses Websense to filter websites. The schools 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 co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing video conferencing

- IP video conferencing 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.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing should be supervised appropriately for the pupil's age.
- Parents and guardians should agree for their children to take part in video conferences.
- Responsibility for the use of the video conferencing equipment outside school time needs to be established with care.
- Only key administrators should be given access to the video conferencing system web or other remote control page available on larger systems.
- Unique log on and password details for the educational video conferencing services should only be issued to members of staff and kept secure.

1.3.8 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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

1.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

## 1.4 Policy Decisions

1.4.1 Authorising internet access

- The schools will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the acceptable ICT user agreement, the E-Safety Agreement Form for School Staff, before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be given a Responsible User Agreement – a copy is also available on the website.

1.4.2 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 Warwickshire County Council can accept liability for the material assessed, or any consequences of internet access.
- The headteacher will ensure that the e-safety policy is implemented and compliance with the policy monitored.

1.4.3 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 headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions will be implemented in line with school behaviour policy and parents will be informed.

Risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence, their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents.

This section will help staff determine what action they can take and when to report an incident of concern to the school's designated child protection co-ordinator or the e-safety officer.

What does electronic communication include?

- Internet collaboration tools: social networking sites and blogs
- Internet research: web sites, search engines and web browsers
- Mobile phones and tablets
- Internet communications: email and instant messaging (IM)
- Webcams and video conferencing
- Wireless games consoles
- MP3 players

What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Bullying and threats
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Identify theft
- Hacking and security breaches
- Corruption or misuse of data

1.4.4 Community use of the internet

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

## 1.5 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

- Rules for the 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 introduced to raise the awareness and importance of safe and responsible internet use.
- AUP signed.

1.5.2 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.
- Policies signed.
- Staff have all received e-safety training from the Local Authority.

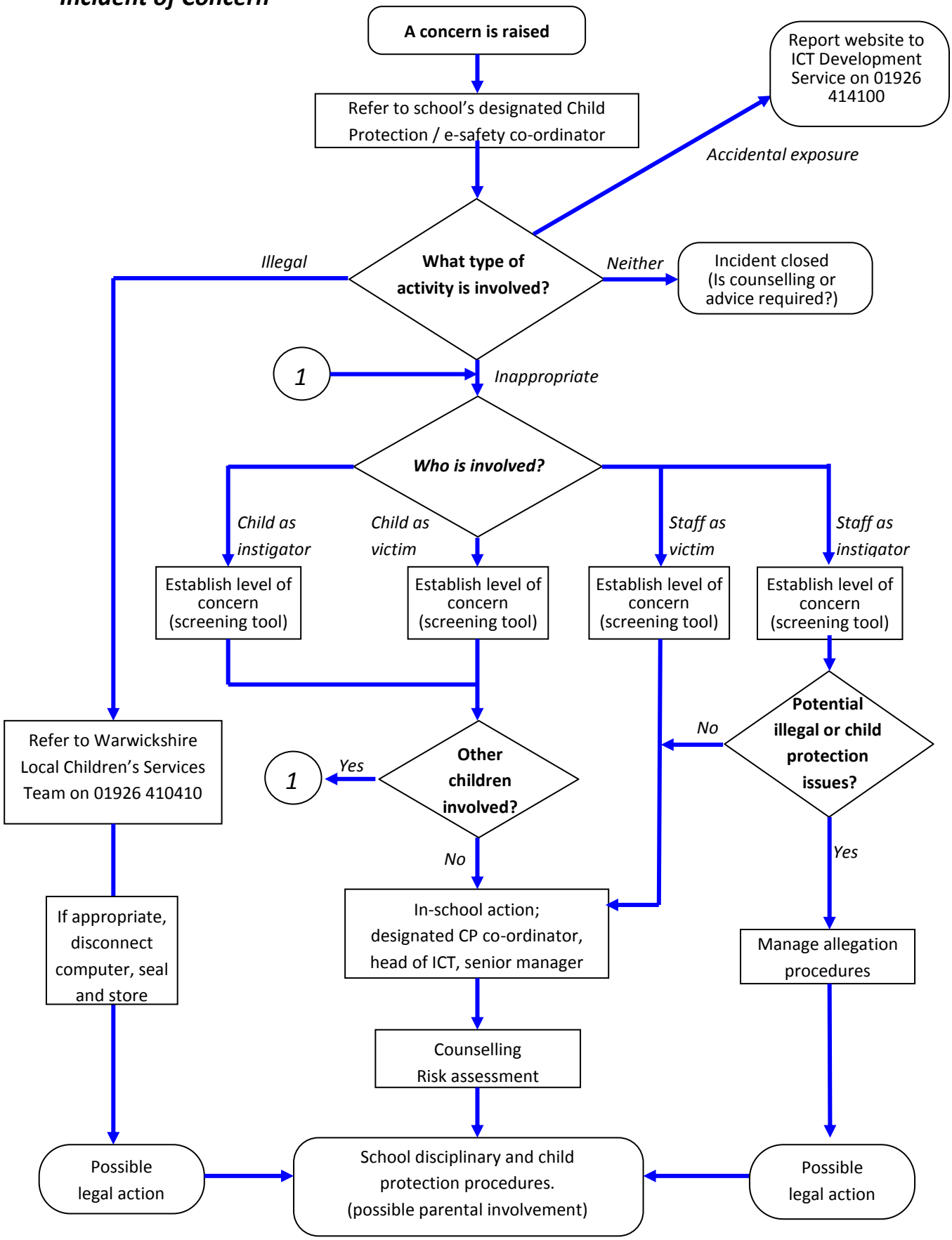
1.5.3 Enlisting parents' support

- Parents' attention will be drawn to the school e-safety policy in newsletters, the school prospectus and on the school website.
- AUP sent home.

Date:

Review:

***Response to an Incident of Concern***



**E-SAFETY CONTACTS AND REFERENCES**

Warwickshire ICT Development Service Desk 01926 414100

360° Safe-Self Review Tool
http://360safe.org.uk/

Safety in Schools and Schools E-Safety Policy
http://www.clusterweb.org.uk?esafety

Schools E-Safety Block
http://www.clusterweb.org.uk?esafetyblog

Child Exploitation & Online Protection Command
http://www.ceop.gov.uk/

Virtual Global Taskforce – Report Abuse
http://www.thinkuknow.co.uk/

Becta
http://nextgenerationlearning.org.uk/safeguarding

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.org.uk/

KidSMART
http://www.kidsmart.org.uk/

NSPCC
http://www.nspcc.org.uk/html/home/needadvice.htm

Childline
http://www.childline.org.uk

NCH – The Children's Charity
http://www.nch.org.uk/stories/index.php?i=324

NCH – Digital Manifesto
http://www.actionforchildren.org.uk/uploads/media/29/5706.pdf

CBBC Safe Surfing including the Chat Guide
http://www.bbc.co.uk/cbbc/help/safesurfing/

Parents' Centre
http://www.parentscentre.gov.uk/usingcomputersandtheinternet