Abbey Church of England Infant and Nursery School

July 2024

E – Safety Policy

In Support of Learning

ICT Development Service

With support from;

Warwickshire County Council

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 computing and for child protection/ safeguarding.

- The school's e-Safety Coordinator is the Headteacher.
- The school has a appointed safeguarding governor who has responsibility for e-safety.
- Our 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, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Teaching and learning

Education

- 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 is a part of the statutory curriculum and a necessary tool for staff and pupils. The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use. These teaching points are delivered in an age appropriate way dependent on the year group.
- Internet access is planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- A planned e-safety programme will be provided as part of our computing curriculum and is be regularly revisited in other areas such as PSHE and in whole school assemblies.
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information
- Rules for the safe and responsible use of ICT systems / internet will be posted in all rooms.
- Staff will guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

- 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 co-ordinator.
- School has a duty to 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 is reviewed regularly.
- Virus protection is installed and updated regularly.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an additional level of protection through its partnership with Warwickshire ICT Development Services. We buy into their internet monitoring and smoothwall filtering service which provides safeguarding alerts and monthly headteacher reports regarding internet use on school equipment. The software captures the screen, identifying machine and user details so appropriate action can

  be taken.
- There are regular reviews and audits of the safety and security of school ICT systems.

E-mail

- •The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access). Any email communications may be monitored in line with the filtering system.

- Pupils may only use approved e-mail accounts on the school system. Pupils are taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate messages and be reminded of the need to write messages clearly and correctly and not include any unsuitable or abusive material. Email will be addressed in Year 2 ICT planning.

Children are taught to follow the rules of Zip it, Block it, Flag it in relation to e-safety.

- Pupils must immediately tell a teacher if they receive an offensive electronic message. (Following the flag it rule)
- Pupils must not reveal personal details of themselves or others in electronic communication, or arrange to meet anyone without specific permission. (Following the Zip it rule)
- Use of words included in the internet monitoring 'banned' list will be detected and logged.
- E-mails and other electronic messages sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. It must be professional in tone and content.
- The forwarding of chain letters or spam is not permitted.

Published content and the school website

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

Please note,

- Pupil's work can only be published with the permission of the pupil and parents.
- Images of staff should not be published without consent.

Social networking and personal publishing

- Social networking sites and newsgroups are not permitted in school.
- Pupils are not permitted 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.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- Staff professional conduct used at all times – staff to read and agree details of this from school safeguarding policy.

Managing filtering

- The school works in partnership with the Warwickshire ICT Development Service to ensure filtering systems are as effective as possible.

- If staff discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing should use the educational broadband network to ensure quality of service.
- Videoconferencing should be supervised appropriately for the pupils' age.

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 phone technology will not be used during lessons or formal school time.
- Staff must not use their own mobile phone when in contact with pupils. Mobile phones and other devises, such as smart watches should only be used during staff break times in staff only areas. Mobile phones and other personal electronic devises should be stored away and out of reach from children during working hours. This is true for all personal electronic devises which can be used for the purpose of communication such as smart watches etc.
- Staff must never use personal electronic devises to take photos of children in school. This includes mobile phones, smart watches or any other personal devise. School equipment should always be used to take photos in school and on school trips. This requirement is clearly set out in the school safeguarding policy. Photos should be stored on school storage systems (staff shared files). They should be deleted once they are no longer needed for education purposes. School equipment is monitored as part of Warwickshire online safety systems. All new software or devices are risk assessed prior to use and appropriate safeguards implemented as necessary.

Protecting personal data

Please refer to the separate detailed Data Protection Policy which will ensure confidentiality of sensitive information relating to staff, pupils, parents and governors.

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff must ensure that they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices – all new laptops are being replaced and are encrypted to protect data.

Policy Decisions

Authorising Internet access

- The school maintains a current record of all staff and pupils who are granted Internet access through acceptable user policies. (AUP’s)
- All users must read and abide by the acceptable ICT use policy before using any school ICT resource.
- In EYFS and Key Stage 1, access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials.
- Visitors are made aware of the E-safety policy and can only access ICT with permission from the Headteacher and being granted a guest log in.

Password Protection

- All users will have clearly defined access rights to school ICT systems.
- Class log ins are used for Lower Key Stage One– their use is always to be supervised and monitored by staff.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

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 takes 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 Headteacher, computing co-ordinator and E-safety governor ensures that the e-Safety Policy is implemented and compliance with the policy monitored.

Handling e-safety complaints

- Complaints of Internet misuse are dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher who should use the agreed WCC procedures.
- Staff are made aware of who to report e-safety incidents to and this information is displayed in the staff room.
- Complaints of a child protection nature are dealt with in accordance with school child protection procedures.
- Pupils and parents are informed of the complaints procedure in the school prospectus.
- Incident logs are to be made where complaints arise, these are to monitored by the E-safety co-ordinator who will review policies to inform future e-safety developments.

Communications Policy

Introducing the e-safety policy to pupils

- Rules for Internet access are to be posted in all networked rooms.
- Pupils and staff are informed that Internet use will be monitored.
- Staff have received training on e-safety. This is updated in staff meetings, training days and school assemblies. It is also updated annually by the E-learning advisor (accredited 360 assessor)
- Induction packs including e-safety guidance and Acceptable user policies are available for new starters and staff.

Staff and the e-Safety policy

- All staff will have access to the School e-Safety Policy and understand its importance.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff e-safety needs are to be audited annually to help to pinpoint support where necessary.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

Enlisting parents' support

- Parents' attention is drawn to the School e-Safety Policy through newsletters, the website and parents meetings.
- The Policy document is available on schoolip for access at anytime.