TEMPLE GRAFTON CHURCH OF ENGLAND PRIMARY SCHOOL
E-Safety Policy

Last Reviewed: Sept 2017
Next Review date: Sept 2019

Contents Page

E-Safety Policy
Temple Grafton C of E Primary School

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.

1. End to End e-Safety

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

- Responsible ICT use by schools including all staff and students, as well as parents, governors and advisers; 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 Central monitoring.

- National Education Network standards and specifications.

Further Information

Warwickshire ICT Development Service   01926 414100

Richard Chapman, E-Learning Adviser   richardchapman@warwickshire.gov.uk

2. Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT and for child protection.

The school's e-Safety Coordinator will be the Designated Child Protection Coordinator as the roles overlap (Mrs Hayton).

- 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, approved by governors and circulated to parents.

- The e-Safety Policy will be reviewed annually.

3. Teaching and learning

1. Why Internet use is important

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.

2. 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.

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 and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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 school e-safety officer.

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 critically aware of the materials they read and shown how to validate information before accepting its accuracy.

4.Managing Internet Access

1. 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 Services.

2. 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.

Whole-class or group e-mail addresses will be used in our primary schools.

E-mail 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.

The forwarding of chain letters is not permitted.

3. Published content and the school web site

The contact details on the Web site should be the school address, e-mail 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.

4. Publishing staff and pupil's images and work

Photographs which 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.

Images of staff will not be published without consent.

5. 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.

Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

6. Managing filtering

The school will work in partnership with the Warwickshire ICT Development Service 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 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.

7. 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 should use a school phone where contact with pupils is required.

8. Protecting personal data

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

5. Policy Decisions

1. 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.

Parents will be asked to sign and return a consent form.

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 WCC can accept liability for the material accessed, or any consequences of Internet access.

The headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

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 who should use agreed WCC procedures.

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 within the school discipline policy include:
– interview/counselling by senior member of staff
– informing parents or carers;
– removal of Internet or computer access for a period.

4. Community use of 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 offer appropriate advice.

6 .Communications Policy

1. Introducing the e-safety policy to 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 introduced to raise the awareness and importance of safe and responsible internet use.

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.

3.Enlisting parents' support

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

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK Kent Grid for Learning (Tunbridge Wells Network)
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search

	Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM Easimail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Kent Grid for Learning Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Skype FlashMeeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum