Stone C of E School

E-Safety Policy

This policy was adopted: Summer 2019

The policy is to be reviewed by Summer 2020

E-Safety Policy

Introduction

The school aims to encourage an understanding of the meaning and significance of faith, and promotes Christian values through the experience it offers to all its pupils.

The school vision is:

'Love one another as I have loved you' (John 13: 34-35)

helping each other to reach for the stars.

The whole community aspire to fulfil this vision through our Christian values of community, perseverance, honesty, compassion, respect and responsibility each being a 'stepping stone' to success.

This policy aims to educate the community about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and devices as well as collaboration tools and personal publishing.

The school's e-safety policy should operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

This policy has been strongly influenced by the work of the Kent e-Safety team.

End to End e-Safety

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 including the effective management of filtering systems

1.0 School e-safety policy

1.1 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.

- The school's e-safety coordinator is also the computing coordinator. She/he works in close co-operation with the headteacher and deputy heads. The headteacher and deputy headteacher are the Designated Child Protection Officers,

- Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors.
- E-Safety issues are included in the Child Protection, Health and Safety, Anti-Bullying, Citizenship and computing policies.
- 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 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.

1.2.3 Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and will include 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.
- Internet access is planned to enrich and extend learning activities.
- Staff 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.

1.2.4 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 the school Computing Coordinator.
- Staff 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.
- Pupils are taught the mechanisms for online reporting
- The school is aware that 90% of radicalisation takes place online. In order to prevent radicalisation and to keep pupils safe we support them to use social media and access to online materials safely in line with our school values and the law.

1.3 Managing Internet Access

1.3.1 Information system security

- The security of the school information systems is reviewed regularly, in conjunction with the support service provider (Turn it On)
- Virus protection is installed and updated regularly.
- The school uses broadband with its firewall and filters.

1.3.2 E-mail

- Pupils, staff and governors may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- 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.
- 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.

1.3.3 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.

1.3.4 Publishing pupil's 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 in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work and their full names can only be published with the permission of the pupil and parents.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. Parents must not publish images of other people's children taken at school events, without permission from the parents.

1.3.5 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.

1.3.6 Managing filtering

- The school will work in partnership with the service provider 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 checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing videoconferencing (Not currently applicable at Stone C of E Combined School)

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- External IP addresses should not be made available to other sites.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' age.

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 are not allowed in school. Any mobile phones brought into school must be deposited with the school office or locked away in lockers. The sending of abusive or inappropriate text messages is forbidden. Staffs' personal mobile phones and devices shall never be used to photograph children.
- Staff have access to a school phone where contact with parents is required

1.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the current data protection regulations

1.4 Policy Decisions

1.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff, including Teaching Assistants and Supply Teachers must read and sign the Acceptable User Policy (AUP) before using any school computing resource.
- At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy.

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.

  The school cannot 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.

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 head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection policy/procedures.
- Pupils and parents should refer to the schools complaints procedure should they have any concerns.

Cyberbullying and Misuse of the Internet

- Cyberbullying or misuse of Internet is unacceptable and will result in sanctions within the school's Behaviour and Discipline policy include. More information can be found in the Social Media policy, anti-bullying policy and Behaviour and Discipline policy.

1.4.4 Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Parents using school IT equipment must sign an AUP consent form prior to use

- Staff and volunteers must not post comments or opinions about the school, children, parents or colleagues, including governors.
- Parents should make complaints through official school channels rather than posting them on social networking sites.

1.5 Communications

1.5.1 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.
- Advice on e-Safety will be introduced at an age-appropriate level as part of curriculum computing sessions to raise the awareness and importance of safe and responsible internet use. The school provides extensive CEOP training for staff and parents, as well as curriculum sessions for all pupils on an annual basis

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.

1.5.3 Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters.

1.6 Sexting

Staff at Stone school are aware that behaviours linked to sexting put children in danger. Such incidents are reported to the Designated Safeguarding Lead and dealt with in line with other policies e.g. Child Protection Policy, Behaviour policy, Anti-bullying policy.

Sexting is the act of exchanging messages, images or videos of a sexual nature through digital communications platforms such as text message, social media or mobile apps. It refers explicitly to self-generated content.

Why do young people sext?

Young people may engage in sexting for a number of reasons, most commonly because they:

- think it is normal, as "everyone else is doing it";
- are in a relationship with the receiver;
- are asked by another to do so, and feel pressurised to please;
- think it is a private exchange between them and the receiver;

- are trying to impress or be perceived as desirable;
- are blackmailed or harassed into it.

What are the consequences?

Sexting is rarely a private, harmless act. Once it has been sent, the sender no longer has any control of where it ends up. If a message is shared, it opens young people up to many forms of abuse or exploitation such as bullying, blackmail and/or public humiliation. In certain cases, legal action may even be taken.

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.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick Picsearch
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.	E schools E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent must be sought prior to publication.	School website
Publishing images including photographs of pupils.	Parental consent for publication of photographs must be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by	School website
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	E schools

Related policies include:

Behaviour and Discipline

Child Protection

Anti-bullying

Social Media Policy