Trusting in God; Growing in Wisdom

Whitegate

CE Primary School

E-Safety Policy

Date: February 2023

Review Date: February 2024

With thankful hearts, we trust in God as we grow in his love which shines through us. We aim to live our faith and grow in wisdom.

Who is wise and understanding among you? Let him show it by his good life, by deeds done in the humility that comes from wisdom. (James 3:13)

But the wisdom from above is pure first of all; it is also peaceful, gentle, and friendly; it is full of compassion and produces a harvest of good deeds; it is free from prejudice and hypocrisy. (James 3:17)

Introduction

E-Safety Subject Leader: Mr M Thomas
Designated Safeguarding Lead: Mrs C Mackenzie
Deputy Safeguarding Lead: Mrs S Ross

1. **E-Safety encompasses Internet technologies and electronic** communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. Whitegate CofE Primary School's E-Safety Policy will operate in conjunction with other policies including those for Relationships, Anti-bullying and the Computing Curriculum.

2. **E-Safety depends on effective practice at a number of levels:**
   2.1. Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
   2.2. Sound implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.
   2.3. Safe and secure internet access including effective management of content filtering.

3. **Why is Internet Use 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. The Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. At Whitegate CofE Primary School we understand the responsibility to educate our pupils in e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

4. **How does Internet Use Benefit Education?**

Benefits of using the Internet in education include:

4.1. access to world-wide educational resources including museums and art galleries;

4.2. professional development for staff through access to national developments, educational materials and effective curriculum practice;

4.3. collaboration across support services and professional associations;

4.4. improved access to technical support including remote management of networks and automatic system updates;

4.5. exchange of curriculum and administration data with the Local Authority;

4.6. access to learning wherever and whenever convenient.

5. **How can Internet Use Enhance Learning?**

5.1. The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.

5.2. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

5.3. Internet access will be planned to enrich and extend learning activities.

5.4. Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils’ age and maturity.

5.5. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

5.6. As pupils progress through the school into Key Stage 2, they will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

5.7. Pupils will be taught how to report unpleasant Internet content.

6. Authorised Internet Access

6.1. The internet access will include filtering provided by Schools Broadband and our firewall will prevent access to any inappropriate sites. Any breaches to security must be immediately reported to the Head teacher, Deputy or E-Safety Subject Leader.

6.2. The school will maintain a current record of all staff and pupils who are granted Internet access.

6.3. User ID and passwords for staff who have left the school are removed immediately or on the last day of their contract.

6.4. Y6 pupils who have left the school are removed from the system during the months of July and August.

6.5. All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource (attached below).

6.6. Parents will be informed that pupils will be provided with supervised Internet access.

7. World Wide Web

7.1. If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the E-Safety Lead who will pass the information on to the Head teacher and network manager.

7.2. Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

8. Email

8.1. The school gives all staff their own e-mail account to use for all school business. This account should be the account that is used for all school business.

8.2. Emails sent to external organisations should be written carefully and proof-read carefully before sending, in the same way as a letter written on school headed paper.

8.3. Staff members' personal email addresses should never be disclosed.

9. Social Networking

9.1. The school will endeavour to block/filter access to social networking sites and newsgroups unless a specific use is approved e.g. Twitter on staff iPads.

9.2. Pupils will be advised never to give out personal details of any kind which may identify them or their location.

9.3. Pupils will not have access to social networking sites at school, but the school will educate pupils in their safe use e.g. use of passwords.

9.4. Pupils will be advised to use nicknames and avatars when using social networking sites.

9.5. Staff must not communicate with students using public social networking sites such as Facebook, Instagram, Twitter, etc.

9.6. Staff should not communicate with parents about school-based issues using public social networking sites such as Facebook, Instagram, Twitter, etc.

10. Filtering

10.1. The network manager will ensure that the filtering systems of the school network are effective.

10.2. All files downloaded from the internet, received via e-mail or on removable media (e.g. Memory Stick) will be checked for any viruses using school provided anti-virus software before files are opened.

10.3. If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the network manager immediately.

10.4. If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Subject Leader or Head teacher, who will inform the network manager.

11. Managing Emerging Technologies

11.1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the Senior Leadership Team before use in school is allowed.

11.2. Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

11.3. If pupils bring a mobile phone into the school this needs to be handed to the school office at the beginning of the day for safekeeping and collected at the end of the school day.

11.4. Tablets are a school tool designed to enhance classroom practice. Children are not permitted to download or access any materials which is illegal, inappropriate or may cause harm or distress to others.

11.5. If staff or pupils discover an unsuitable Apps on the school tablets, it must be reported to the E-Safety Subject Leader, who will inform the network manager.

12. Publishing Pupils' Images and Work

12.1. On a pupil's entry to the school, parents/carers will be asked to give permission for their child's photos to be used in a variety of ways. The purpose will be clearly explained and agreed including Learning Journeys, display and Twitter. Parents must give specific consent for photographs to be used in newspapers, magazines etc. This consent will be considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

12.2. Parents/carers may withdraw permission, in writing, at any time.

12.3. Pupils' full names will not be used anywhere on the Website and Twitter, particularly in association with photographs.

12.4. The school will request that any photos/images taken by parents during whole school events, such as concerts and sports day, will be for their personal use only and not be published on the internet including social networking sites.

13. Information System Security

13.1. School ICT systems capacity and security will be reviewed regularly. Virus protection will be installed and updated regularly.

13.2. The information system security covers fixed and mobile Internet; school PCs, laptops, iPads and digital video equipment. It should also be noted that devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, iPads, tablets, Kindles) are subject to the same requirements as technology provided by the school.

14. Protecting Personal Data

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

14.2. Teachers may carry data on memory sticks or other removable data carriers in order to access their files both at home and at school. Any data carried in this way must be encrypted using appropriate encryption software, e.g. TrueCrypt.

15. Handling E-Safety Complaints

15.1 Complaints of Internet misuse will be dealt with by a senior member of staff.

15.2 Any complaint about staff misuse must be referred to the Head teacher.

15.3 Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

15.4 Complaints of Internet misuse will be dealt with by a senior member of staff.

15.5 Pupils and parents will be informed of consequences for pupils misusing the Internet.

16. Communication of Policy

16.1. Pupils

16.1.1. E-Safety information and posters linking to assemblies delivered by the E-Safety Subject Leader will be posted around school, especially in toilet area and near laptop and iPad lockers.

16.1.2. Pupils will be informed that Internet use will be monitored.

16.1.3. As the pupils progress through the school, children will be taught these SMART tips (from Childnet International – www.childnet.com):

Safe – Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

Meeting – Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

Accepting – Accepting e-mails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable – Information you find on the Internet may not be true, or someone online may be lying about who they are.

Tell – Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online. You can report online abuse to the police at www.thinkuknow.co.uk

16.2. Staff

16.2.1. All staff will be emailed the school E-Safety Policy and its importance explained.

16.2.2. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

16.2.3. All staff will read, fill out and sign the 'Staff Acceptable ICT Use Agreement'

16.3. Parents

16.3.1. Parents' attention will be drawn to the school E-Safety Policy in newsletters and on the school website. The designated E-Safety Leader will provide this information to be added to the newsletter.

16.3.2. Parents' attention will be drawn to the resources and reading provided about E-Safety on the school website. The designated E-Safety Leader will ensure information and resources suggested are up to date.

17. Monitoring and Review

17.1. The E-Safety Policy will be reviewed annually by the E-Safety Subject Leader.

17.2. E-Safety Subject Leader to deliver termly KS1 E-Safety assemblies using the Digiduck resources created for 3-7 year olds.

17.3. E-Safety Subject Leader to deliver termly KS2 E-Safety assemblies using the UK Safer Internet Centre's resources for 7-11 year olds.

17.4. My Online Life E-Safety Scheme of work to be delivered in classes by teachers.

Staff Acceptable ICT Use Agreement

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's E-Safety policy for further information and clarification.

• I will promote E-Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

• I will ensure that my information systems use will always be compatible with my professional role.

• I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.

• I understand that the school may monitor my information systems and Internet use to ensure policy compliance.

• I will respect system security and I will not disclose any password or security information to anyone other than an appropriate authorised person.

• I will not install any software or hardware without permission.

• I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

• I will respect copyright and intellectual property rights.

• I will report any incidents of concern regarding children's safety to the school E-Safety Lead or the Designated Safeguarding Lead

• I will ensure that any electronic communications with pupils and parents are compatible with my professional role.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system

may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
I have read, understood and agree with the Information Systems Code of Conduct.

For safeguarding reasons, parents and pupils should not be added to friendship groups on social networking sites. Apps, such as ‘Messenger’ and ‘WhatsApp’ should not be used to communicate with parents. Members of staff should not ‘follow’ parents from their personal or class Twitter Accounts. Staff should not be friends with parents on Facebook unless there is an exceptional circumstance, which must be declared to the Head teacher. Please fill in the table below to declare social media friendships due to exceptional circumstances.

Name of friend:	Social Media Platform:	Exceptional Circumstance:

Signed: ………………………………….. Capitals: …………………………………..

Date of Policy: February 2023

PERSON RESPONSIBLE FOR POLICY:	***MIKE THOMAS***
APPROVED:	***07.02.23***
SIGNED:	***R CHARLTON***
TO BE REVIEWED:	**FEBRUARY 2024**