Weston Turville CE School

MISSION STATEMENT –
TO PURSUE WISDOM WITHIN A CHRISTIAN ETHOS

E-Safety Policy

Co-ordinator	Mrs L Mercer
Policy produced by	Mrs L Mercer
Policy Agreed	Autumn 2014
Revised	Spring 2019
Next Review Date	Spring 2023

This e-safety policy has been developed by the e-safety co-ordinator and in consultation with the whole school community has taken place through a range of formal and informal meetings.

The e-Safety Policy will be reviewed 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.

As eSafety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

E-Safety in the Curriculum

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 and to help in raising standards. Benefits include access to world-wide educational resources and access to experts in many fields for pupils and staff. Parents will therefore be informed that pupils will be provided with supervised Internet access.

We must also be aware that pupils have access to the internet outside of school in many forms, including computers, mobile phones and other devices.

The school's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils through Turniton. In addition to this staff will be responsible for guiding pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use. They will also be educated on the dangers of technologies outside of school.

The school will ensure pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

The evaluation of on-line materials is a part of every subject. Pupils will be taught to critically evaluate materials and learn effective searching, retrieval and evaluation skills through cross curricular teacher models, discussions and via the Computing curriculum.

Email

The use of e-mail is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette. In order to fulfil the curriculum requirements pupils must have experienced sending and receiving e-mails.

Staff

- Turniton gives all staff their own e-mail account via gmail to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or

malicious e-mails and avoids the risk of personal profile information being revealed.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff must inform (the Computing Coordinator) if they receive an offensive e-mail.
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

Pupils

- Pupils are introduced to e-mail at an age appropriate level.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. These accounts may be accessed if there is suspicion of it being used in an inappropriate manner.
- All pupil e-mail users are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

Staff and Pupils

- It is the responsibility of each account holder to keep the password secure. The school email account should be the account that is used for all school business and is not for personal use
- The forwarding of chain letters is not permitted in school.

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section

- e-mailing Personal, Sensitive, Confidential or Classified Information
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- If you are required to send an e-mail from someone else's account, always make the recipient aware.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly
- Never open attachments from an untrusted source; consult the Computing coordinator first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

e-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible.
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted.
- Where your conclusion is that e-mail must be used to transmit such data:
  - Obtain express consent from the headteacher to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
    - Do not use full names, pictures with names or other easily identifiable information
  - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

Published content

The contact details on the website should be the school address, e-mail and telephone number. Pupils' personal information must not be published. Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Written permission from parents or carers will be obtained before images of pupils are electronically published.

Social networks

The school's filter will block access to social network sites however it is important to be aware that this is often not the case outside school. The school will therefore teach children never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended and e-mail addresses, full names of friends, specific interests and clubs etc.

All children at the school are below the recommended age for using many aspects of social media and they will be taught this in the curriculum. We accept, however, that pupils may still use these and gaming platforms and it is therefore essential to teach them about safe use.

Pupils will 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 (with an awareness that everything can ultimately be shared). Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school. Pupils should be aware of the dangers of location tags which can inform unknown individuals as to their whereabouts.

Pupils will 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. They should also be taught about the use of privacy setttings.

The school is aware that bullying can take place through social networking . Pupils are therefore taught how to seek help in this situation by discussing their issues with an adult or if necessary using the CEOP's safety centre (http://www.ceop.police.uk/safety-centre/) which will be displayed on the school's website. In severe circumstances they are also taught about the role of the police. They are taught to save evidence which can be used at a later date if necessary.

The school also sends out literature to parents from time to time and prints articles in the school newsletter about social media and gaming with signposting to websites and organisations as appropriate.

Social Messaging Services

Staff and pupils are advised as to safe use of social messaging services. These should be used in the same manner as email and social media. No identifiable information should ever be sent even within a closed group. Identifiable photos of pupils should not be shared using social messaging. Closed staff groups should be used in an appropriate and professional manner. Information shared on staff groups should not be shared with external individuals.

Mobile Phones

Personal mobile phones are not to be used anywhere in the school grounds apart from the staff room. They should not ever be used for taking photos of pupils within the school.

Please see the school's mobile phone policy for further information.

Violent Extremism

The internet is a platform where children are at risk of radicalisation. All sites are monitored and extremist sites are blocked when found. Staff and pupils are expected to alert senior staff if they notice suspicious material when online.

New technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupil's mobile phones will not be allowed within school. Staff

telephone numbers will never be provided to parents or children, and staff will never use children's mobile phone numbers as a method of contact.

Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school, Turniton or BucksCC can accept liability for the material accessed, or any consequences resulting from Internet use. If pupils see inappropriate content they are advised to cover the screen and then tell an adult.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Misuse

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.

If pupils deliberately or accidentally access or download unsuitable materials schools should follow the following procedure:

- The screen should be covered immediately and an adult told so that they can switch it off if appropriate
- Any printed materials or disks should be confiscated
- The pupil's access to the Internet should be suspended
- Any further action should be in line with the School's behaviour policy e.g. informing parents.
- The machine should be cleared of any stored unsuitable material before being used by another user

Turniton, as system manager, should audit user areas on networks to reveal large graphic files with, for example GIF or .JPG extensions or with names with series of meaningless letters and numbers.

Communicating the Policy

Pupils

- Children within KS2 will agree to the school's acceptable use policy for pupils.
- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- E-safety will be taught in Computing and throughout the curriculum.
- Whole school assemblies on e-safety will happen when appropriate.
- Pupils may use websites such as grid club (www.gridclub.com) within school to help with learning about e-safety in a safe environment.

Staff

- New staff receive information on the school's acceptable use policy as part of their induction. This is done through signing the netsmart agreement.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.
- Staff training in safe and responsible internet use and on the school e-safety policy will be provided annually.

Parents

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters and on the school website.
- Links to useful organisations for interested parents will also be made clear on the school website.
- A parent's information evening will be provided each year for parents wishing to learn more about e-safety

Appendix 1

Junior NetSmart Code of Practice

I'm NetSmart because at school and at home:

- ✓ I only use the Internet when supervised by a teacher or adult
- ✓ I keep personal information and pictures private
- ✓ I keep my password private and don't use anyone else's.
- ✓ I always tell my teacher/parent if I see bad language or distasteful things while I'm online.
- ✓ I never arrange to meet anyone in person without a parent/ teacher.
- ✓ I leave a chatroom if someone says something which makes me feel uncomfortable or worried, and always report it to my teacher.
- ✓ I ignore nasty, suggestive or rude e-mails or postings and report it to my teacher/parent.
- ✓ I will not look for bad language or distasteful things while I'm online
- ✓ I am always myself and do not pretend to be anyone or anything I am not
- ✓ I know that my teacher and the Internet service provider will check the sites I have visited!
- ✓ I understand that I will not be able to use the Internet if I deliberately look at unsuitable material
- ✓ I understand that information on the Internet may not always be reliable and sources may need checking. Web sites may be sponsored by advertisers

---

Weston Turville CE School

Name of Pupil _____ Class _____

I have read the Pupils' NetSmart Code of Practice and I have discussed it with my son/daughter/ward. We agree to support the school's policy on the use of the Internet.

Signed (Parent/Guardian/Carer) _____ Date _____
Signed (Pupil) _____ Date _____

Appendix 2

Infant NetSmart Code of Practice

I agree that at home and school I will:

- ✓ Only use the computer with an adult in the room
- ✓ Only open pages which an adult says are OK
- ✓ Only use my own password
- ✓ Tell an adult if anything makes me feel scared or uncomfortable
- ✓ Keep my name, age, address and family information to myself
- ✓ Keep photos to myself
- ✓ Not load photos of myself onto the computer
- ✓ Never agree to meet a stranger

Weston Turville CE School

Name of Pupil _____ Class _____

I have read the Pupils' NetSmart Code of Practice and I have discussed it with my son/daughter/ward. We agree to support the school's policy on the use of the Internet.

Signed (Parent/Guardian/Carer) _____ Date _____
Signed (Pupil) _____ Date _____

Staff NetSmart Code of Practice

- Staff closely monitor and scrutinise what their pupils are accessing on the Internet including checking the history of pages.
- Computer monitor screens are readily visible for staff, so they can monitor what the pupils are accessing.
- Pupils have clear guidelines for the content of e-mail messages, sending and receiving procedures.
- Pupils only use the Internet when supervised by a member of staff or adult.
- Pupils are taught skills and techniques to enable efficient and effective use of the Internet.
- Pupils have a clearly defined focus for using the Internet and e-mail.
- If offensive materials are found the monitor should be switched off, any printed materials or disks should be confiscated and offensive URLs should be given to the IT Co-ordinator who will report it to the Internet Service Provider (IFL).
- Virus protection is essential, as viruses can be down loaded accidentally from the Internet.
- The recommended ISP will check sites visited by schools.
- Participating in Newsgroups/discussion groups - these groups are open to all ... therefore be careful! It is recommended that pupils don't use these open forums.
- Personal use of the internet and email is not allowed by any staff.
- Staff should not share personal information or information about the school or staff online publicly through social networking etc and should never accept a pupil or parent as a 'friend' online.

Weston Turville CE School

Name of Teacher _____

I have read the NetSmart Code of Practice for pupils and teachers. I agree to abide by the Teachers' Code of Practice.

Signature _____ Date _____