Winslow Church of England School

E-Safety Policy

Approved by:	Governors	**Date:** March 2021
Last Reviewed on :		
Next Review due by:		

Our vision is ‘Let your light shine’. The rainbow symbolises God’s unconditional love for each individual. We seek to reflect that light in all we do: in our community, both local and wider, our communication, both word and action, with curiosity and courage, and with care and compassion for everyone, inspiring a love of learning.

The purpose of Internet use in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school’s management information and business administration systems. Internet access is an entitlement for students and the school will provide students with a safe and secure Internet access as part of their learning experience.

Benefits of using the Internet in education include:

- Access to world-wide educational resources.
- Educational and cultural exchanges between pupils world-wide.
- Access to experts in many fields for pupils and staff.
- Exchange of curriculum and administration data with Buckinghamshire Council and the Department for Education
- Access to learning wherever and whenever convenient.

The school’s internet access is designed expressly for primary pupil use and includes filtering appropriate for the age of the children through Bucks/Updata.

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. Staff will guide pupils in on-line activities to support the learning outcomes planned. Pupils will be educated in safe and effective use of the Internet. The school will ensure that copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Electronic communication

We use the Internet and e-mail, and we have a school website.

All school members may communicate with others through the Internet. There are many benefits, but also a number of possible dangers. Safeguards in our school include constant adult supervision, sites being filtered by our service provider and controlled links.

The Internet may be used in lessons 'live' for lesson content and for interactive teaching programs.

Our school website provides information about the school, and an opportunity to celebrate children's work with the worldwide learning community.

Managing Information Systems

The security of the school information systems will be reviewed regularly by the Computing Coordinator. Sophos virus protection is installed on all computers and this will be updated regularly. Personal data sent over the Internet will be encrypted and secured. Portable media such as memory sticks and CD-ROMs will not be permitted without specific

permission followed by virus check. Files held on the school's network will be regularly checked and system capacity will be reviewed regularly.

E-mail Accounts

E-mail is an essential means of communication for both staff and pupils. The school uses SIMS ID Outlook e-mail accounts and pupils are only permitted to use class group approved e-mail accounts with adult supervision. Pupils must immediately tell a teacher if they receive offensive e-mail. Access in school to external personal e-mail accounts is blocked. Staff and pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone. Given the age of our pupils at Winslow they are not permitted to use e-mail communications without adult supervision. E-mails sent to external organisations 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.

Website

The school website is designed to celebrate pupils' work, promote the school and provide a portal for communication between school and parents and the wider community. Contact details on the school website include the school's address, e-mail and telephone number. Staff and pupils' personal information must not be published. The head teacher takes overall editorial responsibility to ensure that content is accurate and appropriate. The website complies with the school's own policy on the creation of school websites.

Images that include children will be selected carefully and will not enable individual pupils to be clearly identified. 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 and pupils' work will only be published with the permission of the pupil and parents. Images of pupils or pupils' work will be removed should this be requested by a parent / carer.

Social Networking

Given the age of the children at Winslow access to social networking sites is blocked. Pupils will be taught 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, e-mail addresses, full names of friends, specific interests and clubs etc. Pupils are not allowed to access chat rooms.

Use of digital and video images

- When using digital images, staff should inform, and educate pupils about the risks associated with the taking, use, sharing publication and distribution of images. In particular they should recognise the risk attached to publishing their own images on the internet, e.g. on social networking sites.
- Members of staff can use school equipment to take photographs/videos to support educational aims, but personal equipment cannot be used for these purposes.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

Pupils should 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. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.

Pupils should be advised on security and deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be advised not to publish specific and detailed private thoughts.

Communication options with parents is a constantly changing situation and as such the future need for school based social media accounts would need to be strictly managed and reviewed by senior leaders. Under no circumstances should any member of staff discuss any aspect of Winslow Church of England School or their professional role on social networking sites other than any future specific school based pages/accounts. Governors should also not discuss any aspect of Winslow Church of England School when using social networking sites.

Staff, parents and pupils should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments. Please refer to the Behaviour and Discipline policy in reference to cyber-bullying of staff, by pupils or parents, as well as peer to peer.

Sexting

The avoidance and dangers of 'Sexting' (sharing of inappropriate images) will only be taught to older pupils of the school unless there is a need identified for younger years.

Steps to be taken by all staff if evidence of Sexting has occurred:

Step 1:

If a device is involved -confiscate it and set it to flight mode or, if not possible, switch it off.

Step 2:

Seek advice - report to your designated safeguarding lead via our normal child protection procedures.

Filtering

Filtering of the school's internet access does not guarantee the safety of the pupils and staff. Bucks/Updata provide the school with a filtering system specifically designed for primary schools which has been designed by educators to suit the age and curriculum requirements of our pupils. If staff or pupils discover unsuitable sites, the URL (web address) must be reported to the Computing Lead or Network Administrator. The school recognises that supervision and education are as important as software solutions in ensuring the safety of pupils and staff using the Internet.

The Bucks network uses **WebScreen** ™ which is an industry-standard system used by a many local authorities.

The school will work with Buckinghamshire Council to ensure that systems to protect pupils are regularly reviewed. If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator. Senior staff will ensure that regular checks are made to ensure

that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF (Internet Watch Foundation: http://www.iwf.org.uk/) or CEOP (Child Exploitation and Online Protection Centre: http://www.ceop.gov.uk/).

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Use of hand held technology (Personal phones and School tablets)

- Members of staff can bring in their own personal mobile device into school. They are to be used outside of class time (break or lunchtimes)
- No pupils are permitted to bring in phones or any other hand held electronic devices unless pre-arranged as a special event.
- We recognise there are occasions when children may need to bring a mobile phone to school. This needs to be requested in writing to the headteacher. If granted, the mobile phone must be placed in a named jiffy bag by parents and this should be handed into reception before the start of the school day.
- Pupils in Year 5 and 6 may bring a mobile Phone to school if they have completed a school mobile phone contract. All mobile phones must be turned off while pupils are o the school site and handed to the class teacher on arrival (see Mobile Phone Policy).
- Any phones found in school bags will be confiscated and parents required to collect these in person.
- The school accepts no responsibility for any loss or damage to a mobile phone whilst the device is on the school premises.
- Staff will have access to a school mobile phone for off site visits when required.

Personal Data

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

Internet Access

Pupil usage is always fully supervised and individual usernames are required to access the Internet. Pupils will be informed that network and Internet use will be monitored. E-Safety rules will be posted in rooms with Internet access. Instruction in responsible and safe use will precede Internet access. Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access - Pupils' NetSmart Code of Practice (Appendix 1). The school will maintain a current record of all pupils who are granted access to the school's electronic communications.

An e-safety training programme is in place to raise the awareness and importance of safe and responsible internet use. At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website. Internet issues will be handled sensitively, and parents will be advised accordingly. A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents. Interested parents will be referred to organisations listed in section 3.0 e-Safety Contacts and References.

All staff will be given the School e-Safety Policy and its application and importance explained. All staff must read and sign the "Teachers' NetSmart Code of Practice" (Appendix 2) before using any school ICT resource. The school maintains a record of all staff that are granted access to the school's electronic communications. Staff will be made aware that Internet traffic is monitored and can be traced to individual users. Discretion and professional conduct is essential. Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

The school will take all possible 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 nor Buckinghamshire Council can accept liability for the material accessed or any consequences resulting from Internet use however, methods to identify, assess and minimise risks will be reviewed regularly. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

How will risks be assessed?

• The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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

Curriculum E – Safety

- E safety is planned into the curriculum across all year groups and is regularly revisited
- Resources on the CEOP' Think U Know' website is a basis for our E-safety.
- Key E-Safety messages should be reinforced through assembly input and informal conversations when the opportunity arises.
- All teaching staff receive advice, training and guidance when required, on an ongoing basis.
- We support the e-safety curriculum with pupils and parents by using the Police CEOP officers to give talks to the school community and workshops with the children.
- We reference parents to the 'Think u Know' website to support their understanding.

E-Safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff, in line with the school's Complaints Procedure Policy. Any complaint about staff misuse must be referred to the Headteacher. This policy will be monitored and reviewed annually to meet the needs of this rapidly changing area. Discussions will be held with the local Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues. Sanctions within the school Behaviour and Discipline policy include:

- Informing parents or carers;
- Removal of Internet or computer access for a period;
- Parents and pupils will need to work in partnership with staff to resolve issues.

SMSC

The way in which we approach the social and moral nature of e-safety in school is planned into our teaching of ICT / Computing.

Date readopted by Governing Body: March 2021

Review Date: Spring 2022

Appendix 1 - Pupils' NetSmart Code of Practice

Appendix 2 - Teachers' NetSmart Code of Practice

Appendix 3 – e-Safety resources

Pupils' NetSmart Code of Practice

I'm NetSmart because:

- ✓ I only use the Internet when supervised by a teacher or adult.
- ✓ I never tell anyone I meet on the Internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- ✓ I never send anyone my picture without permission from my teacher/parents/carer.
- ✓ If I am given a password I will never pass it on to anyone, even my best friend.
- ✓ I never arrange to meet anyone.
- ✓ I never hang around in an Internet chat room or in a Usenet conference if someone says or writes something which makes me feel uncomfortable or worried, and always report it to my teacher.
- ✓ I never respond to nasty, suggestive or rude e-mails or postings in Usenet Groups I always report it to my teacher.
- ✓ I always tell my teacher if I see 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 misuse it.
- ✓ I understand that information on the Internet may not always be reliable and sources may need checking. Web sites may be sponsored by advertisers.

Pupil's
Name:……..…

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)

Teachers' NetSmart Code of Practice

- Teachers 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 the teacher, 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 teacher 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 will be confiscated and offensive URLs will be given to the Computing Lead or Network Administrator who will report it to the Internet Service Provider (BCC).
- Virus and malware protection is essential, as viruses can be downloaded accidentally from the Internet. Pupils bringing work from home, on a memory stick, could also infect the computer –Beware
- 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.

I have read the NetSmart Code of Practice for pupils and teachers.

I agree to abide by the Teachers' Code of Practice.

Name:……..

Signed:…….…….. Date:……

Appendix 3 - E Safety Resources

Sexting info for schools

http://swgfl.org.uk/magazine/Content/Documents/Online-Safety/Managing-Sexting-Infographics-designs.aspx

The UK Safer Internet Centre and SWGFL have produced a really useful factsheet for schools: 'Responding to Sexting'. The guidance sets out areas for consideration when deciding whether to report the matter to the police or not. This is currently a difficult area for schools and any advice is helpful.

Website: www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/

Updated SWGFL sexting Guidance

http://swgfl.org.uk/magazine/Managing-Sexting-Incidents/Sexting-Advice.aspx

UKCCIS Guidance for managing sexting in schools/colleges

https://www.saferinternet.org.uk/blog/new-sexting-guidance-schools-released-uk-council-child-internet-safety

NSPCC Sexting Guidance https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/sexting-advice-professionals/

Generic resources for schools

- **Primary** https://www.internetmatters.org/schools/primary/
- **CEOP** resource 5-7 yr olds

https://www.youtube.com/watch?v=-nMUbHuffO8

- **Facebook as a means of communicating with parents**

eSafety Adviser, Alan Mackenzie, has prepared a very thorough guide to 'Facebook as a School Communication Tool' which you can download here

www.esafety-adviser.com/facebook

- **Sharing on line**

https://www.youtube.com/watch?feature=player_detailpage&v=9uJOXOAQ9Qo

- **Advice for helping children set up a new profile**

The UK Safer Internet Centre shares advice for parents and carers when helping their child set up a profile on a new site or game. Key points include: using a family email address; not using personal information (full name or date of birth) in a username; and making sure that profile pictures don't include personal information clues such as school uniforms and house or street names

UK Safer Internet Centre

- **Tackling cyberbullying**

YoungMinds shares a film made by BA students of the Met Film School as part of the YoungMinds vs Online pressures campaign, which shows the effects of cyberbullying as well as a positive way for young people to help their friends by reaching out to them online.

Source: YoungMinds **Date:** 15 June 2016

http://www.youngminds.org.uk/news/blog/3368_reaching_out_and_tackling_cyberbullying

- **NSPCC**

NSPCC launches PANTS song and animation to help protect children from sexual abuse

I am writing to provide you with an update on the NSPCC PANTS campaign. The latest development, which we launched at the end of last week, is the PANTS song and animation. You can view this on the NSPCC website:

www.nspcc.org.uk/pants

You can also see it on You Tube

https://youtu.be/fn6AVSZk008

- Teaching resources – Download Share Aware teaching resources for use in the classroom.

- **Sexualised behaviours**
  Brook: Sexual Behaviours Traffic Light Tool
  https://www.brook.org.uk/our-work/category/sexual-behaviours-traffic-light-tool

- **Consent is everything**
  Video: Tea and Consent
  http://www.consentiseverything.com/

  Alright Charlie
  Resource from the Blast Project aimed at 9 - 11 year olds highlighting the warning signs of grooming in an age appropriate way.
  Video: https://www.youtube.com/watch?v=UGEgn767XAk
  For Pupils: Alright Charlie Workbook
  For Staff: Professional Guidance
  Other Resources: http://www.mesmac.co.uk/projects/blast