West Winch Primary School
E-Safety Policy 2017

This policy should be read in conjunction with our Safeguarding Policy and Computing Policy

Teaching and Learning

Why Internet and digital communications are 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 curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by ICT Solutions and includes filtering by UpData, which is 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.
- Pupils will be educated in the effective use of the Internet
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will seek to 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 will be taught how to report unpleasant Internet content to staff.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive unacceptable e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff to pupil email communication (as part of the curriculum) must only take place via a school email address and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

Publishing photographs, images and work

- Pupils' full names will not be used on the school website, including via social media, particularly in association with photographs.
- Written permission from parents or carers is always obtained before photographs or images of pupils are published
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- Staff will not keep images of children on personal devices e.g. memory sticks, or use them for any use other than in school.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
- Pupils, parents and staff will be advised on the safe use of social network spaces
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work in partnership with Norfolk Children's Services and UpData to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to a member of staff.

- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- If used, pupils should ask permission from the supervising teacher before making or answering a videoconference call.

- If used, videoconferencing will be appropriately supervised for the pupils' age.

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.

Other devices

- Mobile phones and associated cameras will not be used during lessons or formal school time. Taking photographs at any time without the subject's consent is prohibited.

- The sending of abusive, offensive or inappropriate material is forbidden.

- Staff should not share personal telephone numbers with pupils and parents (a school phone is provided for staff where contact with parents is required).

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource (see Appendix 1).

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school, Norfolk Children's Services or UpData can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit ICT use to establish if this E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective

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 and will be dealt with through the Governing body complaints procedure if required.

- Complaints of a child protection nature must be referred to the Designated Safeguarding Lead (DSL) and dealt with in accordance with school child protection procedures.

Communicating E-Safety

Introducing the E-Safety policy to pupils

- Appropriate elements of the E-Safety policy will be shared with pupils

- Pupils will be informed that network and Internet use will be monitored

- Curriculum opportunities to gain awareness of E-Safety issues and how best to deal with them will be provided for pupils

Staff and the E-Safety policy

- All staff are made aware of the latest E-Safety guidelines and policy – and regular training updates are provided.

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

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

Enlisting parents' support

- Parents' and carer's attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school web site.

- Parents and carers will from time to time be provided with additional information on E-Safety.

- Parents and carers will be reminded that they must not publish any images of or comments about performances and other community events on social media.

Adopted: Spring 2017
Review: Spring 2019

Heather Habbin - Chair of Governing Body

Appendix 1

West Winch Primary School
Staff Code of Conduct for ICT

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all adult users are aware of their responsibilities when using any form of ICT. All such users are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with school management or the ICT Subject Leader.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras; email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is an offence to use a school ICT system and equipment for any purpose not permitted by its owner.
- I will only use the school's email/Internet and any related technologies for uses permitted by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username
- I will ensure that all school generated electronic communications are appropriate and compatible with my role.
- I will only use the approved, secure email system(s) for any school business
- I will ensure that all data is kept secure and is used appropriately and as authorised by the Head Teacher or Governing Body. If in doubt, I will seek clarification. This includes taking data off site.
- At school, I will not install any hardware or software without the permission of the ICT Subject Leader or Leadership Staff.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images will only be taken, stored and used for purposes in line with school policy and with written consent of the parent, carer or adult subject. Images will not be distributed outside the school network without the consent of the subject or of the parent/carer, and the permission of the Head Teacher.

- I understand that my permitted use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the ICT Subject Leader or Head Teacher.

- I will respect copyright and intellectual property rights.

- I will not jeopardise the safety or wellbeing of any child or adult in the school through my use of ICT.

- I will report any incidents of concern regarding children's safety to the Senior Designated Professional or Head Teacher.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full name _____ (please print)

Role _____

Signature _____ **Date** _____