



Wonersh and Shamley Green Church of England Primary School

Guildford Road
Shamley Green
Surrey
GU5 0RT

Tel: 01483 892345
Fax: 01483 892391

Email: info@wsg.surrey.sch.uk
Web site: www.wsg.surrey.sch.uk

Headteacher: Mrs Tess Trewinnard MA NPQH

INTERNET SAFETY POLICY

Policy written: January 2014

To be reviewed: Spring 2016

VISION AND VALUES

“In an exciting, challenging and safe environment, children and staff feel happy and valued and are encouraged to become independent, confident and enthusiastic learners.”

This policy acts as guidance to all members of our community in the safe use of the internet to support children’s learning. Some guidance may be more appropriate for older pupils, but is still relevant in the context of the wider community.

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 children 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 to enhance their learning in all subjects across the curriculum
- The school Internet access is provided by Surrey County Council and includes filtering appropriate to the age of pupils
- Pupils will be taught about acceptable Internet use; be educated in the effective use of the Internet, including the skills of research, retrieval and evaluation
- 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 are shown how to validate information before accepting its accuracy.
- Pupils will be taught about the acceptable use of the internet and how to report unpleasant Internet content e.g. telling an adult, using the whistle blowing tool on our Learning Platform, CEOP Report Abuse icon or Hector Protector.

MANAGING INTERNET ACCESS

Information system security

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

Email

- Pupils and staff may only use approved e-mail accounts on the school system.
- Accounts should be protected using strong passwords.
- Pupils must immediately tell a teacher if they receive offensive e-mail. Staff should inform the Headteacher or Chair of Governors.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication will only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- E-mail from pupils to external bodies will be monitored by class teachers.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names will not be used on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The school will seek to use group photographs rather than full-face photos of individual children.
- Parents will be informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

- The school will monitor access to the learning platform, and consider laying good foundations for the safe use of social networking sites e.g. use of passwords
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils must not store personal photos on the school learning platform
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils
- Pupils will be advised to use nicknames and avatars when using social networking sites

Managing filtering

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher or IT technician.
- Regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Video conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Video conferencing will be appropriately supervised by the class teacher.

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
- Games machines including the Sony Play station, Microsoft Xbox and others have Internet access which may not include filtering. These are not currently used in our school.
- Staff will use a school phone where contact with pupils is required.
- The appropriate use of our Learning Platform will be discussed within school

Acceptable use of personal devices by pupils

- Mobile phones and personally used devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices (ipads, tablets etc).
- The Bluetooth functionality of a mobile phone should be switched off at all times and may not be used to send images or files to other mobile phones.
- Mobile phones and personally owned devices may not be used during lessons or formal school time. They should be switched off at all times.
- The sending of abusive or inappropriate text messages is forbidden.
- If a pupil needs to contact his parents/carers they will be allowed to use the school phone.
- Parents are advised not to contact their child via their mobile phone during the school day but to contact the office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils may use school devices for specific learning activities under the supervision of a member of staff.
- Pupils breaching the school policy will have the phone or device confiscated. It will be held in a secure place in the school office and only released to parents/carers in accordance with the school policy.

Acceptable use of personal devices by staff

- Staff are not permitted to use their own mobile phones or devices for contacting pupils or those connected with the family of the student, except in emergencies on school trips.
- Mobile phones and personally-owned devices should be switched off or switched to silent mode.
- Bluetooth communication should be hidden or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by the Senior Leadership Team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and should only use school provided equipment for this purpose.
- Staff use of mobile phones during the school day will normally be limited to break times and after school.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Staff should never contact students from the personal mobile phone or give their mobile phone number to students. If a member of staff needs to make telephone contact with a parent, a school telephone should be used.
- Staff should never send, or accept from anyone, texts or images that could be viewed as appropriate
- If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff must not keep any personal data or photographs on laptops that leave the school or on their personal phones.
- Personal data should be stored only on the school network or the School Learning Platform (password protected)

POLICY DECISIONS

Authorising Internet access

- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials
- All staff must read and sign the “Acceptable Use of ICT Guidelines” before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- Parents will be asked to sign and return a consent form
- Any person not directly employed by the school will be asked to sign an “Acceptable Use of ICT Guidelines” before being allowed to access the Internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the Internet Safety policy is adequate and that the implementation of the Internet Safety policy is appropriate and effective.
- Pupils will be taught to use the internet responsibly and report to their teacher anything that causes them concern and any inappropriate use by other pupils.

Handling Internet Safety complaints

- Complaints of Internet misuse will be dealt with by the Head teacher
- 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 procedures
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Internet Safety policy.

COMMUNICATIONS

Introducing the Internet Safety policy to pupils

- Appropriate elements of the Internet Safety policy will be shared with pupils
- Internet Safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of Internet Safety issues and how best to deal with them will be provided for pupils

Staff and the Internet Safety policy

- All staff will discuss the importance of the School Internet Safety Policy
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff should consider carefully their use of social networking sites and behave in a responsible and professional manner which does not bring the school into disrepute.

Enlisting parents' support

- Parents' and carers attention will be drawn to the School Internet 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

- The school will ask all new parents to sign the Home School agreement when they register their child with the school.

In our school the Internet Safety coordinator is the Head teacher, who is also the Designated Child Protection Coordinator.

- Our Internet Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors
- The Internet Safety Policy and its implementation will be reviewed annually

This policy should be read alongside all school policies but relates especially to the following policies and documents:-

The School Development Plan
Learning and Teaching Policy
ICT Policy
Home Learning Policy
Anti – Bullying Policy
Child Protection and Safeguarding Policy
The Home School Agreement
Acceptable Use of the Internet Guidelines

Useful Links

Child Exploitation & Online Protection Centre

<http://www.ceop.gov.uk>

The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children. Their education arm runs the “Thinkuknow” programme and website.

Key SCC contact:

LADO Local Authority Designated Officer and quality Assurance Manager.

Geraldine Allen

email: Geraldine.allen@surreycc.gov.uk

Tel: 01372 833321

A list of useful links to Internet Safety resources can be found on the Internet Safety pages of the Surrey ICT Leaders Portal: <http://www.surreylearning.co.uk>



ACCEPTABLE USE OF ICT

Guidelines for Staff & Volunteers

These guidelines cover the use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the approved, secure email system(s) for any school business
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Head teacher
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I understand that all Internet usage / and network usage can be logged
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.
- I will not use personal digital cameras or camera phones for transferring images of pupils or staff without permission.
- I will use the school's Learning Platform in accordance with school advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities.
- I will ensure any confidential data that I wish to transport from one location to another is password protected using encrypted storage.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

I agree to follow the guidelines outlined and abide by the school Internet Safety Policy

NAME:

Signed:

Date:



USING THE INTERNET

Internet Safety Guidelines for Pupils

It is the responsibility of the class teacher to discuss these guidelines with the children in their class and ensure they are followed. We also ask parents to discuss them at home and support the school in the safe use of the internet.

Keeping safe: Stop, think, before you click!

- ✓ I will only use ICT in school for my own learning.
- ✓ I will only use my class email or my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or approved by my teacher.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own personal details such as my name, phone number or home address.
- ✓ I know that my use of ICT can be checked, and that my parent/ carer will be contacted if a member of school staff is concerned about my safety.



Dear Parent / Carer,

Information Communication Technology (ICT), including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using ICT.

Our Internet Safety policy can be found on the school's web site or a copy obtained from the school office.

Please read and discuss the accompanying Internet Safety guidelines with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your child's class teacher or myself.

Yours sincerely,

Mrs Tess Trewinnard

Head teacher



Parent / Carer signature

I grant permission for my child /children to have access to use the Internet, e-mail and other ICT facilities at school.

We have discussed the Internet Safety guidelines and

(child name) agrees to follow the Internet Safety guidelines and to support the safe use of ICT at Wonersh and Shamley Green CofE Primary School. We will support this at home.

Parent/ Carer Signature

Date

Wonersh and Shamley Green C of E Primary School
Guildford Road, Shamley Green, Surrey GU5 0RT
T. 01483 892345 F. 01483 892391
E: info@wsg.surrey.sch.uk
W: www.wsg.surrey.sch.uk