DORMER HOUSE SCHOOL

E-Safety Policy

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and **Safeguarding**. The ICT co-ordinator will undertake the role of e-safety officer and will work closely with the Designated Safeguarding Leads, the Senior Leadership Team and the Trustees to review this policy annually.

The school acknowledges that the Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.

The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information to a wider audience.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy. Pupils will be taught how to report unpleasant Internet content.

Managing Internet and E-mail Access

- School ICT security will be reviewed by our service provider.
- Virus protection will be updated regularly.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and only published with the permission of parents or carers.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, 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.
- Pupil image file names may refer to the pupil by first name only.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which might identify them, their friends or their location.
- Ideally pupils would use only moderated social networking sites, e.g. SuperClubs Plus
- 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 with NS Optimum 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 e-Safety Coordinator.
- Senior staff will ensure that ICT support staff make regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use 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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- **Mobile phones will not be used by staff, volunteers or visitors during lessons or in the presence of children.**
- Mobile phones may be used within the staffroom.
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Staff should use a school phone where contact with pupils/parents is required.
- Mobile phone cameras must not be used on the school site or trips either by pupils or members of staff **unless permission has been specifically granted by the Headteacher.**

Protecting personal data

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

Authorising Internet access

- All staff must read and sign the Staff Code of Conduct for ICT 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 annually.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources 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, owing to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- 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 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 Head Teacher.
- Complaints of a child protection nature must be reported to the Designated Child Protection Officer and will be dealt with in accordance with school child protection procedures.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety e.g. Computer Explorers.

Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- All pupils will sign an e-safety code of conduct. This will be done by the class teacher with the younger having read and discussed the contents of the code of conduct
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed in liaison with Gloucestershire Constabulary
- E-Safety training and education will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Enlisting the support of parents and carers

- Attention will be drawn to the School e-Safety Policy in newsletters, the Parent Handbook and on the school website.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Useful resources for teachers

BBC Stay Safe - www.bbc.co.uk/cbbc/help/safesurfing/
Chat Danger - www.chatdanger.com/
Child Exploitation and Online Protection Centre - www.ceop.gov.uk/
Childnet - www.childnet-int.org/
Cyber Café - http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen - www.digizen.org/
Kidsmart - www.kidsmart.org.uk/
Think U Know - www.thinkuknow.co.uk/
Safer Children in the Digital World - www.dfes.gov.uk/byronreview/

Useful resources for parents

Care for the family - www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD - http://publications.teachernet.gov.uk
Family Online Safe Institute - www.fosi.org
Internet Watch Foundation - www.iwf.org.uk

Parents Centre - www.parentscentre.gov.uk
Internet Safety Zone - www.internetsafetyzone.com

This policy is monitored by the Headteacher and the Trustees and will be reviewed annually.

Signed **Date:**