Dormers Wells Junior School E-Safety Policy

Philosophy

At Dormers Wells Junior School, we believe that Information and Communications Technology (ICT) expands horizons, by shrinking worlds and with this in mind it contributes to the school curriculum in many ways:

→ It prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology

→ Pupils use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination

→ Pupils learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures

→ Increased capability in the use of ICT promotes initiative and independent learning, with pupils being able to make informed judgements about when and where to use ICT to best effect, and to consider its implications for home and work both now and in the future

We have updated this policy in line with the changes to data protection which came into law in May 2018. This policy relates directly to our data protection and freedom of information policies and our privacy notice

Teaching and learning

Why the 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 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. Under the revised 2014 primary curriculum, computing is a core subject.

Internet use will enhance learning

→ The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. London Grid for Learning provides screening for inappropriate content and this is monitored weekly by our ICT technician.

→ 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 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.

Pupils will be taught how to evaluate Internet content

→ 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 e.g. using the CEOP Report Abuse icon.

Dormers Wells Junior School E-Safety Policy

Managing Internet Access

Information system security

- School ICT systems security is reviewed regularly by the computing technician and Yosabe
- Virus protection will be updated regularly.
- Security strategies will be discussed with the DPO and Headteacher

E-mail

- Pupils may only use approved e-mail accounts on the school system and follow the rules as given in the acceptable use policy.
- 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 generally be published. The contact details given online should be the school office.

Publishing pupil’s images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. We will use group photographs rather than full-face photos of individual children. It is good practice to compress images and resize to ensure misuse.
- Pupils’ full names will not be used on a school website or other on-line space, particularly in association with photographs.
- Parents will be given the right to refuse the publishing of images that include their child. Written notice must be made and we will remind parents of their right regarding this matter. On admission parents will be asked for consent
- Likewise if a parent wishes that their child’s work is not published then we will respect the parent/carers wish. Written notice must be given.
- Pupil image file names will not refer to the pupil by name.
- 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 not allow access to social networking sites, but we will 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 may identify them, their friends or their location.
- Ideally pupils would use only moderated social networking sites, e.g. Moshi Monsters
- 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 Becta 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 regular checks are made 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 are NOT permitted in school and therefore will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- The appropriate use of Learning Platforms or VLE will be taught in lessons and the e-safety website used to train pupils in the safe use. The preferred VLO for the school is My USO
- The VLE will not allow external messaging access. Only approved users will use the VLE and therefore will have a username and password that will not be shared by others. ***SEE VLE SECTION BELOW.***

Protecting personal data

- Personal data will only be recorded, processed, transferred and made available according to the General Data Protection Regualtions May 2018

Virtual Learning Environments

Usage

- It is permitted that the virtual learning environment may be used within or outside of the school.
- The site is accessible through the internet and it must be acknowledged by all that use the site that this is the case.
- For security, all usage is monitored by school and therefore messages and content are logged. The acceptable use policy must be agreed before children are permitted to access the VLE.

Submitting content

Any content uploaded must not contain any of the following:

→ Swearing or rude language in either censored or uncensored form.

→ Slander or abuse in any form, jokingly or not.

→ Rude images.

→ Repeated or nuisance messages.

→ Advertisement for any services, goods or events outside of the School, without being given prior permission by the ICT Management.

→ Personal or private details of users.

→ Content that could interfere with examination or marking.

→ Viruses, ad-ware or malware of any form that could do damage to another user's PC.

→ Anything that may offend others.

Care must be applied when posting. What qualifies any of the above in is the joint judgment of the moderators and staff members?

→ All content is subject to normal school polices that apply to staff or pupils at the time of being submitted. As such, forum discussion will be treated as it was spoken within the school grounds.

→ Users must own the rights to the content they submit and where necessary must refer to the original source fairly and legally. By agreeing to this policy you accept liability for any content you submit.

Visibility

→ All users of the site must be aware that areas of the site may be publicly accessible to non- authenticated users outside of the school. Though the best effort will be made by the administrators to ensure that the privacy of users is kept.

→ User account password must be kept private, though it is acceptable for parents or guardians to use the same account. Students are expected to ensure that their parents read and agree to the acceptable use agreement before being allowed to use that student's account. No other person apart from the staff, registered guests, students, parents or guardians may login to the VLE.

→ If a user is aware that their login user name and password has been compromised they must immediately contact a member of staff to have the account password changed.

Banning

→ Failure to abide to this policy may result in a ban for the offending user.

→ The user may have certain user privileges removed for a set or unlimited amount of time rather than a complete ban. The length and scope of the ban is subject to the offense and is to be decided by an administrator.

→ The duration of the ban is subject to the nature and extent of the offense and to be the decision of an administrator.

Moderation/Teacher accounts

→ Users will be informed if they have been assigned as moderators.

→ Moderators must actively ensure that the rules outlined in this policy document are abided by, within their jurisdiction, by all users, including each other and staff.

- If a moderator does not abide by this policy document or misuses their moderator privileges, those privileges will be removed and the moderator may be subject to a ban. Administrators will judge what is considered as misuse.
- Users who believe that a moderator is misusing their privileges on the VLE must report it to an administrator.
- In the event of posted content breaching this agreement moderators must:
- Delete the content (i.e. a forum message) or edit it in order to censor the sensitive content.
- Warn the user (by posting a message or emailing them).
- If the incident is severe alert the e-safety co-ordinator or a senior member of staff immediately.
- A note of the offense under the user name should be noted to the database in the moderator section.

Updates

- In the event that this policy document is updated users will be informed. In this event the user will be presented with the updated policy when logging on next and asked if they agree with the amended version.

Unauthorised access

- If a user finds that they do not have the correct user privileges they must report this to the moderator immediately.
- Any signs of unauthorised access onto the virtual learning environment must be reported to an administrator immediately. This includes a person using another person's user name and password to log in.

General Policy Decisions

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.
- 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, due 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 cann ot 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 headteacher.
- Complaints of a child protection nature must 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.

Dormers Wells Junior School E-Safety Policy

Communications Policy

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; children will sign a contract regarding internet safety
- 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, possibly based on the materials from CEOP, Mark Robinson will advise on a scheme of work
- e-Safety training will be embedded within the ICT scheme of work, the Personal Social and Health Education (PSHE) curriculum and will be of priority when accessing the internet for cross-curricular use .

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 that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils and should pre-test any site that has not been used before.

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- 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.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK The school / cluster VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail Kent Learning Zone Cluster Microsite blogs
Publishing pupils‟ work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils‟ full names and other personal information should be omitted. Pupils‟ work should only be published on „moderated sites‟ and by the school administrator.	Making the News SuperClubs Plus Headline History Kent Grid for Learning Cluster Microsites National Education Network Gallery

publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learning grids Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils‟ work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives “On-Line” Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers

BBC Stay Safe www.bbc.co.uk/cbbc/help/safesurfing

Becta http://schools.becta.org.uk/index.php?section=is

Chat Danger www.chatdanger.com

Child Exploitation and Online Protection Centre CEOP 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

Kent e-Safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/e-safety_home.cfm

Kidsmart www.kidsmart.org.uk
Kent Police – e-Safety
www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html

Think U Know www.thinkuknow.co.uk

Safer Children in the Digital World www.dfes.gov.uk/byronreview

Appendix 3: Useful resources for parents and carers

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

Writing and reviewing the e-safety policy

Dormers Wells Junior School E-Safety Policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection. Due to the emerging technologies this policy is always under review.

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.
- Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy was revised by: Julia Taylor
- It was approved by the Governors on:
- The next review date is January 2019