WEST BOROUGH

PRIMARY SCHOOL

E-SAFETY POLICY

Chair of Governors	Mr T Barker
Date agreed	September 2014
Headteacher	Mrs A Crittenden
Review date	September 2016

This policy has been adapted from Kent's E Safety Policy, 2007 and the current Kent online policy generator information. It should be noted that many of the statements included are 'Kent' statements and must be stringently applied in the work at West Borough Primary School. At West Borough Primary School the E Safety Officer role is part of that of the Designated Child Protection Coordinators and ICT leader. The ICT Leader must work closely with the Designated Child Protection Coordinators as the roles may overlap in the case of E Safety. Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors and staff.

Teaching and learning

- Why Internet use is important

The Internet is an essential element in all aspects of life, including 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 statutory curriculum and a necessary tool for staff and pupils.

- 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. 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 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

- Information system security

School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed with Kent.

- E-mail

Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission from the teacher / responsible adult. E-mail sent to an external organisation 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. Whole-class or group email addresses should be used in primary schools.

- Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The headteacher 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 will not enable individual pupils to be clearly identified. Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs. Written permission is obtained from parents regarding use of images.

- Social networking and personal publishing

The school will block/filter access to social networking sites. 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 or their location.

- Managing filtering

The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it 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

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Pupils should ask permission from the supervising teacher before making or answering a videoconference call. 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. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Staff will be issued with a school phone where contact with pupils is required.

- Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The quantity and variety of data held on pupils, families and staff is expanding rapidly. While this data can be very useful, it could be mishandled, stolen or misused.

The following points are taken form the Data Protection Act 1988. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data in which people can be identified is protected.

<u>Policy Decisions</u>

- Authorising Internet access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The school will keep these as a record of all staff who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. All staff also must read and sign our ESafety Rules document.

- Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is 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. Pupils and parents will be informed of the complaints procedure.

Communications Policy

- Introducing the e-safety policy to pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored. Each year group follows a unit of work that specifically teaches about e-safety.

- Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Enlisting parents' support

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

e-Safety Contacts and References

Schools ICT Security Policy
http://www.eiskent.co.uk (broadband link)

e-Safety in Schools and Schools e-Safety Policy
http://www.clusterweb.org.uk?esafety

Schools e-Safety Blog
http://clusterweb.org.uk?esafetyblog

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk/contact–us.html

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

Think U Know website
http://www.thinkuknow.co.uk/

Becta
http://www.becta.org.uk/schools/esafety

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

Kidsmart
http://www.kidsmart.org.uk/

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Childline
http://www.childline.org.uk/
Stop Text Bully
www.stoptextbully.com
NCH – The Children's Charity
http://www.nch.org.uk/stories/index.php?i=324
NCH – Digital Manifesto
http://www.nch.org.uk/uploads/documents/Digital–Manifesto–web.pdf
BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Appendix: 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 Kent Grid for Learning (Tunbridge Wells Network)
Using search engines to access information from a range of websites.	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.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM EasyMail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
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.	Making the News SuperClubs Infomapper Headline History Kent Grid for Learning Focus on Film
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.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
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 Skype FlashMeeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum

Acceptable Usage Policy

SOFTWARE

Only licensed software may be installed onto school laptops & computers.

Software currently installed on the laptop computer includes the following:

- Microsoft Internet Explorer
- Microsoft Word
- Microsoft Power Point
- Microsoft Excel

Teachers are not authorised to install unlicensed software on computers. If a teacher requires special or non-standard software to be installed on laptops for school use, it must be cleared by the ICT Leader/ICT Technician beforehand. The teacher will be responsible for supplying licenses, media, and any documentation. Licence information is a requirement of the County Auditors.

Breach of these conditions may lead to disciplinary action.

1. For network connection of laptops, users are provided with a dedicated account. The user is to use no other account on the network. The user should at all times keep any passwords for this account secure and private. The user takes full responsibility for the use or misuse of this account.
2. This account allows the user certain privileges and rights on the network. The user should in no way attempt to gain other privileges or to attempt to access resources on the network to which no explicit rights have been granted.
3. The user shall not in any way, tamper or misuse school equipment, either software or hardware. No form of tampering is acceptable.
4. Laptops can have access to the Internet. Abuse of this access, in the form of access to pornographic sites is absolutely forbidden. Please note that access to certain pornographic sites may be in serious breach of the law (Child Trafficking and Pornography Act 1998). The school will fully co-operate with the relevant authorities in investigating and prosecuting any such illegal access.
5. E-mail and Internet chat rooms, where these relate to their Schoolwork or study, should be used in a courteous manner, respecting the etiquette of the network. Usage of any form of profanity in these communications is absolutely forbidden.
6. Users may not download copyrighted software, audio or video files, or any other copyrighted material from the Internet. Any such material found will be deleted without prior notification.
7. Software in use in the School is licensed in a correct and legal manner. However (except where explicitly stated), it is not available to users for home usage. Users should make no attempt to copy licensed or copyrighted material from the School network.
8. The facilities are for School related educational use only. The facilities are not available for use on external projects or for work activities not associated directly with courses or the School. Facilities may not be used for any form of personal financial gain.
9. The contents of all mailboxes, PCs, server shares and caches operated by the School, remain the property of the School. The status of these data

stores is similar to that of letters posted to the School to a post holder (not marked as personal and private).

10. E-Mail should be considered as an insecure medium for the transmission of confidential information. Where confidential information is to be transferred, in particular externally, it should be done in an encrypted form.
11. Notwithstanding that every effort is made to ensure that home folders and e-mail are secure, the School does not in any way guarantee the security of this data.
12. Food and drinks should be kept well away from laptops. The user should also take care when shutting down and closing the lid of laptops to ensure that nothing is left lying on top of the laptop surface. This may result in damage not covered by warranties, in which case the user will be liable for repair costs.

Guidelines for User Responsibilities:

Use of West Borough Primary School ICT resources is granted based on acceptance of the following specific responsibilities:

- Use only those computing and information technology resources for which you have authorisation.
  For example: it is a violation
  - to use resources you have not been specifically authorised to use
  - to use someone else's account and password or share your account and password with someone else
  - to access files, data or processes without authorisation
  - to purposely look for or exploit security flaws to gain system or data access
- Use computing and information technology resources only for their intended purpose.
  For example: it is a violation
  - to send forged email
  - to misuse Internet Relay Chat (IRC) software to allow users to hide their identity, or to interfere with other systems or users
  - to use electronic resources for harassment or stalking other individuals
  - to send bomb threats or "hoax messages"
  - to send chain letters
  - to intercept or monitor any network communications not intended for you
  - to use computing or network resources for advertising or other commercial purposes
  - to attempt to circumvent security mechanisms
- Protect the access and integrity of computing and information technology resources.
  For example: it is a violation
  - to release a virus or worm that damages or harms a system or network
  - to prevent others from accessing an authorised service
  - to send email bombs that may cause problems and disrupt service for other users

  - to attempt to deliberately degrade performance or deny service
  - to corrupt or misuse information
  - to alter or destroy information without authorisation
- Abide by applicable laws and university policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
  For example: it is a violation
  - to make more copies of licensed software than the license allows
  - to download, use or distribute pirated software
  - to operate or participate in pyramid schemes
  - to distribute pornography to minors
  - to upload, download, distribute or possess child pornography
- Respect the privacy and personal rights of others.
  For example: it is a violation
  - to tap a phone line or run a network sniffer without authorisation
  - to access or attempt to access another individual's password or data without explicit authorisation
  - to access or copy another user's electronic mail, data, programs, or other files without permission

Computing and E-Safety Rules at West Borough Primary School
September 2014

The following is a reminder of what we allow / do not allow at West Borough Primary School:

- **No children are allowed on computers**, either in classrooms or the IT Suite **without adult supervision**. The **teacher** is ultimately **responsible** for computer use, even when another adult is supervising children.
- Staff or pupils' personal information (eg address) will not be published on our website.
- Photographs that include pupils 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.
- The school will block / filter access to social networking sites. **Pupils** will be advised **never to give out personal details** of any kind which may identify them or their location.
- If **staff or pupils** discover an **unsuitable site**, it must be **reported to the ICT leader or the IT technician immediately.**
- Videoconferencing will be appropriately supervised at all times.
- **Mobile phones will not be used during lessons** or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Protecting personal data - Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The quantity and variety of data held on pupils, families and staff is expanding rapidly. While this data can be very useful, it could be mishandled, stolen or misused. **Data will be: Processed for specified purposes; Adequate, relevant and not excessive; Accurate and up-to-date; Kept secure; Held no longer than is necessary.**
- Any **data or images onto personal phones, cameras or laptops** will be **downloaded immediately after use / a visit, and deleted from personal and / or portable equipment**. This includes assessment data (spreadsheets).
- **E-safety rules** will be posted in all networked rooms and **discussed with the pupils at the start of each year and regularly throughout the year. Pupils will be informed that network and Internet use will be monitored.**
- **Email – there should be no communication with pupils or parents from personal email addresses. School ones must be used (ending: @west-borough.kent.sch.uk).**
- **Social Networking** – staff **must not add a child (past or present)** as 'friend'. **We strongly recommend that parents are not added** as 'friends' either.
- **Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.**

I have read and understand the above rules. I acknowledge that they are an important part of Safeguarding children.

Signed………………………………………… Date……………………………