WANSDYKE PRIMARY SCHOOL
E-safety Policy

Status	Date
Staff	March 2016
Q and S sub committee	March 2016
Revision due	Autumn 2018

Rationale
The use of ICT by children and staff is integral to both the administration and teaching and learning at Wansdyke Primary School. As technologies develop, we must ensure that all of our community are kept up to date. Underpinning all this, needs to be an understanding of safe practice, when on-line, that ensures that we minimise risk. All e-safety incidents (and near misses) are recorded in the ICT Coordinator's e-safety log (e.g. Appendix 1). Staff are asked to report any incidents in every staff meeting. This policy works alongside the PSHE and Bullying policy.

School Responsibilities
The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator, who is also the ICT Leader. Alice Hall is the current appointee. The school E-safety Coordinator will work alongside the Designated Child Protection Coordinator in the case of any incident. Michelle Tett is the current appointee. Where possible, an E-safety governor will be elected (which may or may not be the Child Protection Governor). Louise Leacy is the current E-safety appointee. An annual e-safety presentation will be made to governors and any policy will be amended before the revision date, if appropriate.

Why is the internet important?
Children:
- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- Pupils use the Internet widely outside school and will need to learn how to access and evaluate online information and to take care of their own safety and security.
- 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 and safe Internet access as part of their learning experience via specific sites and search engines.
- It allows access to world-wide communication, information and resources that have been filtered for children.
- It allows access to carefully chosen games to motivate and develop learning

Staff (including Governors) :
- It enables the exchange of curriculum and administration data with (LA) and DfE;
- It facilitates administration tasks
- It enables communication with parents, children and the wider community, through our website.

How are the risks managed?
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.
- Neither the school, nor LA, can accept liability for the material accessed, or any consequences resulting from Internet use. However, this policy has been created to minimise the risk.
- Lessons are delivered to raise awareness of staying safe online (see below)
- E-safety issues will be actively addressed through the PSHE and ICT curriculum covering both school and home use, and a 'safe to tell' approach about cyberbullying is in place across the school.
- E-Safety 'SMART' 'rules will be posted in all classrooms and as the wallpaper to computers and laptops.
- Pupils will be informed that network and Internet use will be monitored.
- A regularly updated e-safety page will provide links to information for parents (and children), and where this is not our own, the source will be acknowledged.

- Instruction in responsible and safe use should precede Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

In addition to lessons, specific e-safety days and events may be organised to raise awareness for children, parents and the wider community.

How will the internet (including e-safety) be taught in lessons?

- Pupils will be regularly taught how to protect themselves online, through assemblies and PSHE lessons, using the Thinkuknow resources (at age-appropriate levels), supplemented with other teaching materials, where appropriate.
- Pupils will be supervised when using the internet and clear age-related learning objectives will be shared for efficient, safe internet research and learning.
- Communications (including passwords and online accounts) will be taught at an age-appropriate level
- Pupils will be given access to unique learning experiences such as the use of live satellite imagery and real time data, exploration of sophisticated models and simulations, contributing to the social construction of knowledge (through the use of wikis, games, blogs and social networks), contact with experts and peers in other locations, creating and sharing of multimedia materials.
- Pupils will be taught to understand that when using Internet material they need to acknowledge the source, and check the validity of the website, as a means of protecting themselves. Staff will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- The 'SMART' E-Safety rules will be displayed in every classroom and referred to at relevant times.

Authorising Internet access

- Parents and pupils will be asked to sign a 'Responsible Internet Use' form.
- All staff and volunteers or placement students must read, understand and sign the school's 'Acceptable Use' form.
- Parents will be informed that pupils will be provided with supervised Internet access.

What filtering is in place?

- The school maintains and supports the managed filtering service provided by LA
- Hectors World dolphin has been loaded onto all computers and pupils are taught how to click this if something comes up which scares or worries them. The teacher will then make a note of the URL, that has come up and report this directly to the e-safety coordinator and the ISP.
- Requests from staff for sites to be removed from the filtered list will be considered by the Head Teacher and IT technician. A record will be kept of these sites and where access has been permitted to them.
- If staff or pupils discover unsuitable sites, the URL must be reported to the (ISP) (0117 9037 999 cyps.it.helpdesk@bristol.gov.uk) and the E-safety co-ordinator will need to log it in the E-safety log.
- Any material that the school believes is illegal will be reported to the LA who provide the Internet Filtering Service.
- The Head Teacher will ensure that regular checks are made to make sure that filtering methods selected are appropriate, effective and reasonable.

Use of e-mail

- Pupils may only use approved e-mail accounts (webmail).
- Teachers will deliver lessons about staying safe when using email (following the SMART rules).
- Children will be taught how to use an appropriate tone in their emails.
- Any reported issues of cyber bullying, via email, will be dealt with, and parents informed.
- (Staff only) E-mail sent to external organisations should be written carefully and ensure that it represents the professional values of the school, in the same way as a letter written on school headed paper.
- (Staff only) The forwarding of chain letters is not permitted.
- (Staff only) The standard disclaimer of 'The views expressed in this email and/or attachments are not necessarily those of the school or LA' will be visible on all emails sent out from the school.

Social networking

- Inappropriate social networking sites are blocked centrally by Bristol LA (at a schools request) and we will seek to teach pupils how to use social networking sites safely through virtual environments.
- Cyberbullying will be treated as bullying, and children/staff will be encouraged to take screen shots as evidence.
- Pupils will be advised how to access social network space out of school safely. They will be warned how public the information is, and taught the SMART rules.
- Pupils should be advised not to publish specific and detailed private thoughts.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

- A Facebook guide for parents will be published on our website.
- Social networking sites can only be unblocked with the specific permission of the Head Teacher, if required.
- Pupils will be advised to never use real photos for profiles (avatars will be encouraged), and they will be educated in the risks of publishing and distributing images.
- Staff and governors are advised to use extreme caution when using social networking sites for personal use and should avoid having parents as Facebook friends: Staff and governors will sign a social networking agreement.
- Teachers will not run social network spaces for pupils' use on a personal basis.

Personal mobile devices (including cameras, smartphones, laptops, netbooks and tablet technology)
- Children's mobile phones should be kept, turned off, in their bags (at the children's own risk).
- The sending of abusive or inappropriate messages is forbidden.
- Children and parents will be asked to only take photos/footage of their own children in association with the school.
- Staff are not permitted to use their own personal devices to record images or footage of children.
- Memory cards, with digital images, should be kept on site (unless on a visit) and uploaded to the server as soon as possible.

Videoconferencing (Sykpe)
- Permission will be sought by the parents if the children are to be involved in a conference call
- Staff will supervise all conference calls and use a class log on, where the password is not shared.

Emerging technologies
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Managing the website
- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The website should respect copywrite restrictions, and remain professional.
- All children will have given written permission to have their photographs posted onto the school website.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Security of the school information systems
- Virus protection will be updated regularly by the School's IT provider.
- Security strategies discussed within Bristol Network meetings, or advice from SWGfL or Bristol Authority, will be implemented where appropriate
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Staff are expected to regularly check portable storage devices for viruses and ensure no confidential data, or photographs are carried on them
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- The ICT subject leader will review system capacity regularly with the Edit technician.
- Personal log ins are provided for teaching, support and administrative staff.
- Staff passwords may not be shared, which will ensure all the sensitive data on staff laptops is protected.
- The Administrator password for the school ICT system, used by the IT technician (or other person) must also be available to the Head Teacher or other nominated senior leader and kept in a secure place (eg school safe).
- SIMS may only be used by authorised staff and must be closed down when not in use

Personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. We will follow the eight Data Protection principles of good practice that underpin the act:
- Personal data shall be processed fairly and lawfully and shall not be processed unless specific conditions are met.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

E-safety complaints

- Complaints of Internet misuse will be dealt with by the Class Teacher, Head Teacher and/or the e-safety coordinator as appropriate, and logged.
- Any complaint about staff misuse must be referred to the Head Teacher.
- The Head Teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with e-safety incidents – included as appendix 2 – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)
- E-safety issues surrounding children or families will be handled sensitively, and parents will be advised accordingly.

Appendix 1
Wansdyke Primary School **E-safety Incident Log**
Details of ALL e-safety incidents (and near misses) to be recorded by the e-safety Coordinator (A. Hall). This incident log will be monitored by the Head Teacher, Member of SLT or E-safety Governor. Any incidents involving Cyberbullying should be reported to the Child Protection officer and suitable policies enforced. Staff meetings minutes will detail the weeks where 'no incidents' were recorded.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

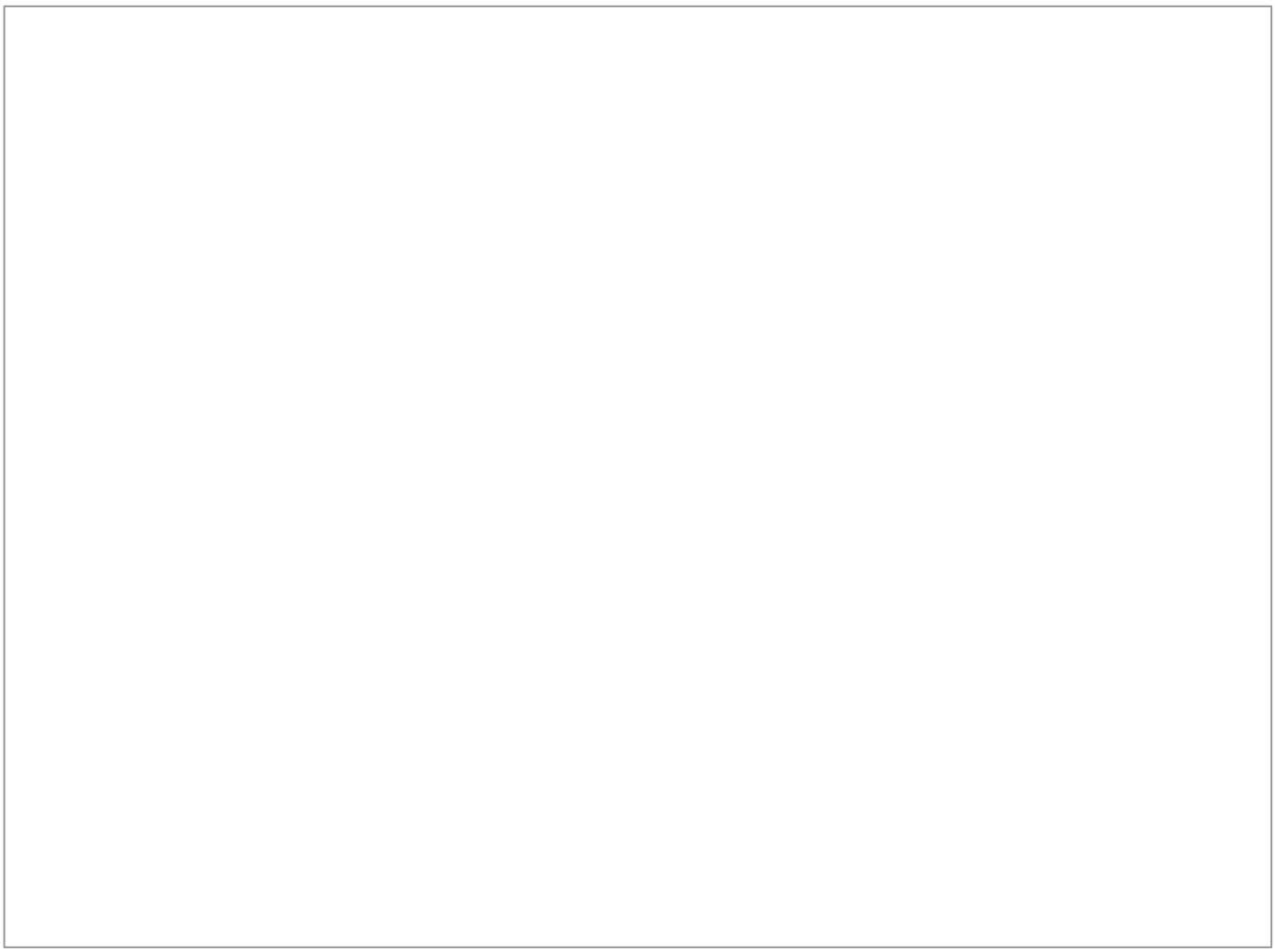
Appendix 2
SWGfl flow chart on dealing with e safety incidents

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows: The forms below confirm our current school approach.