Wooden Hill Primary and Nursery School

E-Safety Policy

Approved by Curriculum committee	Summer 2015
Approved by Governing Body	Summer 2015
Responsibility for implementation and review	ICT Co-ordinator
Date of next review	Summer 2018
Linked to:	Anti-Bullying Policy Acceptable Use Document
To be read by	All
Outcome:	Ensuring the safety of all

Abbreviations:

Wooden Hill Primary School

E-Safety Policy

Our e-safety policy has been written by the school, building on, Bracknell Forest LA ICT Advisory Group recommendations and government guidance. It has been agreed by the senior management, and approved by governors following discussions with all staff members and school council. It will be reviewed annually.

Why is internet use important?

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

How will internet use enhance learning?

- The school internet access is designed expressly for pupil and staff use and does include filtering appropriate to the age of pupils.
- Pupils will be taught about their responsibilities towards acceptable use of the internet and electronic communications.
- Internet access will be planned to enrich and extend learning activities through a wide variety of curriculum subjects. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, evaluation and retrieval.
- Pupils will have access to a secure blog to enable them to collaboration about aspects of their learning

How will pupils learn to evaluate internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via our ICT technician.
- Schools will ensure that the use of internet derived materials by staff and by pupils complies with copyright law. (See appendix on the use of images)
- Pupils in KS2 will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils in Year 5 & 6 will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

How will electronic communications be managed ensuring safety for pupils?

- 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 details of themselves or others in e-mail communication or via a personal web space, such as address or telephone number, or arrange to meet anyone.
- Personal email or messaging between staff and pupils will not take place.
- Whole-class or group e-mail addresses should be used.
- Access in school to external personal e-mail accounts may be blocked for pupil and staff who do not comply with the acceptable use policy.
- Social e-mailing will not occur unless appropriate for specific learning to take place. In this situation a member of staff will approve all emails.
- E-mail sent to an external organisation should be written carefully and authorised by a member of staff before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Children may blog through the restricted community site each post is approved by a member of staff.

How should the school website content be managed?

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site 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.
- Written permission from parents or carers will be obtained on entry to the school, before photographs of pupils are published on the school website.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce it has been obtained.

Newsgroups, e-mail lists and forums

- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.
- Access to forums that are moderated by a responsible person or organisation and are directly linked to an educational activity will only be permitted through secure login processes and where the teacher has completed a risk assessment of the forum.

Chat and instant messaging

- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will not have access to social networking sites using the school network.
- Children should use only regulated educational chat environments and the school blog. This use will be supervised and the importance of chat room safety emphasised.
- Any form of bullying or harassment is strictly forbidden and all children will be encouraged to raise any issues of cyber bullying with any adult in school. All incidents of cyber bullying will be investigated in the same way as other incidents of bullying following our anti-bullying procedure.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school. This assessment will be kept in a folder in the ICT suite.
- **Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, social networking sites, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement**

of a line manager should be sought first and appropriate professional language should always be used.

Personal websites and blogs

- Pupils will not have access to social networking sites using the school network
- When publishing material to websites and elsewhere, pupils should consider the thoughts and feelings of those who might view the material. Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable.

Photographic, video and audio technology

- When not in use, video conferencing cameras should be switched off and turned to face a wall.
- It is not appropriate to use photographic or video devices in changing rooms or toilets.
- Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.
- Staff may use only the school cameras or video cameras to take digital images to support school trips and curriculum activities.
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.
- Pupils should always seek the permission of their teacher before making audio or video recordings within school.

How can emerging ICT applications be managed?

- 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 school hours.
- The sending of abusive or inappropriate text messages is forbidden.
- Mobile phone cameras should not be used inappropriately and photographs should not be forwarded to unknown sources.
- The use of blog messaging may only happen on the school blog which has restricted access and approved posting technology.

How will internet access be authorised?

- The school will keep a record of all staff and pupils 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. Staff and pupils are aware that internet access may be monitored.
- At Key Stage 1, access to the internet will be directly supervised to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised internet access .
- Pupils will not be issued individual email accounts, but will be authorised to us a group/class email address under supervision.

How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. 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 Bracknell Forest Borough Council can accept liability for the material accessed, or any consequences of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored.
- Access is strictly forbidden to any websites that involve gambling or financial scams .

How will filtering be managed?

- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via our ICT technician.
- Following advice from SEGfL, the Headteacher, ICT technician and ICT co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.org.uk).
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

How will e safety be introduced to the children?

- Rules for internet access will be posted in all rooms where computers are used.
- Pupils will be informed that internet use will be monitored.
- Instruction in responsible and safe use should always precede internet access.
- Regular opportunities will be provided through both ICT lessons and PSHE lessons to discuss and raise awareness of the issues surrounding e-safety both within the school environment and out off the school environment.
- Children will know what to do and who to tell if they discover something inappropriate or offensive on a website in school.

How will staff be consulted and made aware of this policy?

- All staff must accept the terms of the 'Acceptable Use' statement before using any internet resource in school.
- All new staff will be taken through the key parts of this policy as part of their induction.
- All new staff will be provided with a copy of this policy.
- All staff including teachers, supply staff, teaching assistants and other support staff, will be provided with the School e-Safety Policy, and have 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.**
- The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures will be supervised by senior management.
- Staff development in safe and responsible internet use, and on the school internet policy will be provided as required.
- Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection is installed and updated regularly via our ICT technician.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- **Personal data sent over the internet will be encrypted or otherwise secured**, and will only take place using the school email.
- Use of portable media such as memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check. Staff must use the secure, locked USB stick they have been provided with for any pupil information.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Staff must seek permission from the ICT technician or the Headteacher prior to loading additional software onto their laptop.
- Files held on the school's network will be regularly checked.
- The ICT technician will ensure that the system has the capacity to take increased traffic caused by internet use.

How will complaints regarding internet use be handled?

- Follow LA guidelines for investigation and response for incidents involving misuse of social networking sites.
- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions available include:
  - interview/counselling by head of year;
  - informing parents or carers;
  - removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies. Advice sought should include how best to preserve any possible evidence.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (web addresses in reference section).

Wooden Hill Primary and Nursery School

Staplehurst
Wooden Hill
Bracknell
Berkshire
RG12 8DB

Tel: 01344 421117
Fax: 01344 305952
Email: head@office.woodenhill.bracknell-forest.sch.uk

Headteacher
Mrs Joanna Quinn MEd

Dear Parents

Responsible ICT Use

As part of your child's curriculum and the development of ICT skills, we provide supervised access to the internet. We believe that the effective use of the internet and e-mail is worthwhile and an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible ICT Use and sign and return the consent form so that your child may use internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe internet access if you wish. We also have leaflets from national bodies that explain the issues further.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, we cannot be held responsible for the nature or content of materials accessed through the internet. We will not be liable for any damages arising from your child's use of the internet facilities.

Should you wish to discuss any aspect of internet use please do not hesitate to make an appointment to meet with me.

Yours sincerely

Joanna Quinn
Headteacher

Wooden Hill Primary School

Responsible Internet Use

Please complete, sign and return to the school office

Pupil:	***Form:***
Pupil's Agreement I have read and I understand the school Rules for Responsible ICT Use. I will use the computer system and internet in a responsible way and obey these rules at all times.	
Signed:	***Date:***
Parent's Consent for Internet Access I have read and understood the school rules for responsible internet use and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.	
Signed:	***Date:***
Please print name:	
Parent's Consent for Web Publication of Work and Photographs I agree that, if selected, my son/daughter's work may be published on the school website. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.	
Signed:	***Date:***

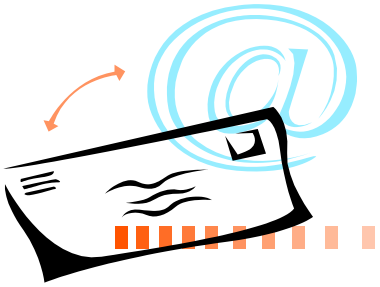
Wooden Hill Primary School

Responsible ICT Use

These rules help us to be fair to others and keep everyone safe.

- **I will ask permission before using the internet.**
- **I will use only my own network login and password, which is secret.**
- **I will only look at or delete my own files.**
- **I understand that I must not bring software or disks into school without permission.**
- **I will only e-mail people I know, that my teacher has approved.**
- **The messages I send will be polite and sensible.**
- **I understand that I must never give my home address or phone number, or arrange to meet someone.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **I will only use the school blog for internet chat.**
- **I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I understand that the school may check my computer files and the internet sites I visit.**
- **I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers.**

This poster must be displayed near all computer workstations in the school.



May 2008 ICT Briefing Note
Regarding: Copyright and school websites/VLEs
Following: BBC website article

There is a particular issue emerging with regard to the use of copyright protected photographs in school web pages, particularly now that robotic software exists that allows copyright holders to search for sites that are using their images. This BBC article dated 13th March 2008, highlights the issue clearly:
http://news.bbc.co.uk/1/hi/education/7283926.stm
To quote this article directly:
"*The problem schools have is that while a lot of images are OK for them to use under the 'education' umbrella, when they out those images on their websites or swap lesson plans with those images in, they are facilitating the free re-distribution of those images and that is where the problems are occurring.*
Copyright lawyer Linda Macpherson said there is a fairly common misconception that material can be freely copied if this is for educational purposes."
In general, all material created by someone else, including graphic images, photographs and text, is subject to copyright legislation, unless the copyright owner chooses to waive their rights. Pupils' therefore own the copyright to any work that they produce and their permission should be obtained before publishing it on a website or VLE.
Where possible, materials for school websites and VLEs should be created internally, because then the school is the copyright holder and can use the materials as it sees fit.
Schools should ensure that staff and pupils are fully aware of the importance of copyright law and that there is the possibility of large financial penalties to the school and/or individual if this is breached. Copyright law should be mentioned in the appropriate school policy, eg. an Acceptable Use of the Internet policy or AUP. One possible statement is *"The use of internet derived materials by staff and by pupils must comply with copyright law."*
Some websites may offer material that is free to download for non-commercial purposes. One site providing images on this basis is http://www.stockvault.net/ . Clipart and photographic collections that can be purchased on CD or DVD usually allow the purchaser to reuse the material on websites, although they may impose conditions in their licence terms.
The Becta website (link below) offers further guidance to schools on copyright and includes this quote, "*Unauthorised use* [of copyright material] *can be a criminal offence, equivalent to theft.*" It also notes an interesting exemption for visually impaired students. "*To support visually impaired students, the Copyright (Visually Impaired Persons) Act 2002 allows copying of hard copy and digital materials to create an accessible format. This might allow, for example, texts to be copied and enlarged for use with access devices in the classroom.*"
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_le_03&rid=9983

Appendix A

Facebook Guidance for Schools (Cyberbulling/Inappropriate Behaviour)

1. If you know the identity of the perpetrator, contacting their parents or, in the case of older children, the young person themselves to ask that the offending content be removed, often works.
2. Failing that, having kept a copy of the page or message in question, delete the content.
3. For messages, the 'delete and report / block user facilities' are found in the 'Actions' dropdown on the page on which the message appears.
4. For whole pages, the 'unfriend and report / block user facilities' are at the bottom of the left hand column. Always try to cite which of the Facebook Terms and Conditions have been violated (see note 10 for the most likely ones) at http://www.facebook.com/terms.php or Community Standards at http://www.facebook.com/communitystandards/. Note that Facebook are more alert to US law than UK. The process should be anonymous.
5. If the page is by someone under 13 click on http://www.facebook.com/help/contact.php?show form=underage (Facebook say they will delete any such page.
6. To remove a post from a profile, hover over it and on the right there will be a cross to delete it.
7. Does the incident trigger the need to inform the policy or child protection agencies?
8. To report abuse or harassment, email abuse@facebook.com (Facebook will acknowledge receipt of your email and start looking into your complaint within 24 hours. They will get back to you within 72 hours of receiving your complaint).
9. If all else fails, support the victim, if they wish, to click the 'Click CEOP' button. The link is found at http://www.thinkuknow.co.uk
10. If the victim is determined to continue using Facebook, they might want to delete their account and start again under a different name. Deletion can be done here https://ssl.facebook.com/help/contact.php?show form=delete account. They should be made aware of the privacy issues that might have given rise to their problem in the first place.

Appendix B

Further Guidance

CEOP (Child Exploitation and 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. That means that they are part of UK policing and very much about tracking and bringing offenders to account either directly or in partnership with local and international forces.

Think U Know

http://www.thinkuknow.co.uk Think U Know is CEOP's support, guidance and resource site for children, young people, parents, carers and adults who work with children and young people.

UK Safer Internet Centre

http://www.saferinternet.org.uk/ This website provides the latest advice on how to use the internet and new technologies safely and responsibly. Also find a range of practical resources, news and events focussing on the safe and responsible use of the internet and new technologies.

Bracknell Forest e-safety webpage

http://bracknell-forest.gov.uk/esafety These pages define e-safety, describe the possible risks and also detail what Bracknell Forest is doing to safeguard vulnerable users of the internet and other digital technologies in the Borough. It also includes useful resources such as leaflets, videos and guidance which can be downloaded and used within organisations/settings to raise awareness of the risks and how to be safe.