Walmore Hill Primary School
E-safety policy

Written October 2015
Review due: October 2016

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to use the technology safely, respectfully and responsibly; to be able to recognise acceptable/ unacceptable behaviour; identify a range of ways to report concerns about content and contact. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones and touch screen tablet devices. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Young people have access to the Internet from many places, home, school, friends' homes, libraries and in many cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe.

This policy is designed to ensure safe internet use by pupils in school, but also while on-line at home etc. The policy will operate in conjunction with other policies including those for Acceptable Use, Behaviour, Bullying, Curriculum, Data Protection and Security.

End to End e-Safety

- E-Safety depends on effective practice at a number of levels:
- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband internet access using RM safety net.

Teaching and learning

Why Internet use is important

- 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.
- 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 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 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.

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.
- 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.

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 from parents or carers will be obtained before photographs of pupils are published on the school Web site, class blog or twitter.
- Pupil's work can only be published with the permission of the pupil and parents.

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.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LEA, DfES 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 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.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff must read the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- 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.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

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.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

While acknowledging the benefits, it is also important to recognise that risk to safety and well-being of users is ever-changing as technologies develop. These can be summarised as follows:

- Commercial (adverts, spam, sponsorship, personal information)
- Aggressive (violent/hateful content)
- Sexual (pornographic or unwelcome sexual content)
- Values (bias, racism, misleading info or advice)
- Contact
- Commercial (tracking, harvesting personal information
- Aggressive (being bullied, harassed or stalked)
- Sexual (meeting strangers, being groomed)
- Values (self-harm, unwelcome persuasions)
- Conduct
- Commercial (illegal downloading, hacking, gambling, financial scams,terrorism)
- Aggressive (bullying or harassing another)
- Sexual (creating and uploading inappropriate material)
- Values (providing misleading info or advice)

Much of the material on the internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism that would be considered ***inappropriate and restricted*** elsewhere.

It is also known that adults who wish to abuse others may pose as a child/young person/peer to engage with them and then attempt to meet up with them. This process is known as ***'grooming'*** and may take place over a period of months using chat rooms, social networking sites and mobile phones.

Cyberbullying is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages or e-mails either personally or anonymously, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e-mail.

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.

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

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.

Appendices

Organisation Staff and Volunteers

This covers use of digital technologies in the organisation i.e. e-mail, internet, intranet and network resources, learning platforms, software, mobile technologies, equipment and systems.

- I will only use the organisation's digital technology resources and systems for professional purposes or for uses deemed reasonable by the manager.
- I will only use secure e-mail system(s) for any organisation's business (web mail accounts are not secure e-mail system(s)).
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access, receipt of inappropriate materials or filtering breaches to the manager.
- I will not allow unauthorised individuals to access e-mail / internet / intranet / networks or systems.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself.
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed.
- I will follow the DSCF 2009 'Guidance for Safer Working Practice for Adults who work with Children and Young People' (http://www.timeplan.com/uploads/documents/Downloads/Safer-Working-Practices.pdf
- I will ensure that my personal e-mail accounts, mobile/home telephone numbers are not shared with children, young people or families.
- I will not allow children and young people to add me as a friend to their social networking site nor will I add them as friends to my social networking site.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I understand that all internet and network usage can be logged and this information could be made available to my manager on request.
- I will not connect a computer, laptop or other device to the network/internet that has not been approved by the organisation and meets its minimum security specification.
- I will not use personal digital cameras or camera phones for transferring images of children and young people or staff without permission.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that the Data Protection Act requires that any information seen by me with regard to staff or children and young people, held within any organisation system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will at all times behave responsibly and professionally in the digital world and will not publish any work-related content on the internet.
- I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice.
- I understand that failure to comply with this Acceptable Use Policy (AUP) could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the organisation’s most recent Acceptable Use Policy (AUP).

I agree to abide by the organisation’s most recent Acceptable Use Policy (AUP).

Signature ……….……………………………… Date ……………………Full Name

…………………………………..….. (print)Job

title..Organisation ....

Facebook Guidance for Schools (Cyberbullying/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 police or child protection agencies?

8. To report abuse or harassment, email abuse@facebook.com (Facebook will acknowledge receipt of you 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 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:

- You will not bully, intimidate, or harass any user (1.3.6)
- You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission (4.1)
- You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law (5.1)

NOTE: An effective education programme can help to reduce the number of times that this sort of incident arises, over the medium term. Such a programme should help young people to match their online behaviour with their offline behaviour by helping them to develop understanding, skills and behaviours in these sorts of areas:

- possible consequences
- understanding the effects of bullying on others
- understanding how technology can magnify impact

- understanding how comments or other actions can be perceived differently by the originator and the target.

The Use of Digital Images and Video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We follow these rules for any external use of digital images:

If the student is named, we avoid using their photograph.

If their photograph is used, we avoid naming the student.

Where showcasing examples of students' work, we only use their first names, rather than their full names.

(The school should make a judgement with the inclusion of the following statement):

If showcasing digital video work to an external audience, we take care to ensure that students are not referred to by name on the video, and that students' full names are not given in credits at the end of the film.

Only images of students in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school

  e.g. in class or wider school wall displays or PowerPoint© presentations.

(The school should make a judgement with the inclusion of the following statement):

- *Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators e.g. within a DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.*

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission e.g. if your child won a national competition and wanted to be named in local or government literature.

The Use of Social Networking and On-Line Media

This school asks its whole community to promote the 3 'common' approaches to online behaviour:

o **Common courtesy**

o **Common decency**

o **Common sense**

How do we show common courtesy online?

o We ask someone's permission before uploading photographs, videos or any other information about them online.

o *We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.*

How do we show common decency online?

o We do not post comments that can be considered **intimidating, racist, sexist, homophobic or defamatory.** This is **cyber-bullying** and may be harassment or libel (i.e. a criminal act).

o When such comments exist online, we do not forward such emails, tweets, videos, etc. to other people/groups. This could be considered criminal behaviour.

How do we show common sense online?

o We think before we click.

o We think before we upload comments, photographs and videos.

o We think before we download or forward any materials.

o We think carefully about what information we share with others online, we check where it is saved and we check our privacy settings.

o We make sure we understand changes in any websites we use.

o We block harassing communications and report any abuse.

<u>NOTE:</u> Any actions online that impact on the school and can potentially lower the school's (or someone in the school's) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social networking sites, this will be addressed by the school in the first instance. However, if necessary, the police may be involved and/or legal action pursued