



# E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

October, 2016  
v4.0

## INTRODUCTION

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy should operate in conjunction with other policies; these are highlighted in the 'Linked Policies' section at the end of this policy

## 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 and agreements (Acceptable Use). (Appendix 2)
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems

## 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 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.
- Internet access will be planned to enrich and extend learning activities.

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them 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

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school e-Safety Coordinator (Headteacher).
- Staff should ensure that the use of Internet derived materials by staff and by 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

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

##### 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, 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. (Appendix 3)

## SOCIAL NETWORKING AND PERSONAL PUBLISHING

- Social networking sites and newsgroups will not be used unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

## MANAGING EMERGING TECHNOLOGIES

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff have access to a school phone where contact with pupils is required.
- Sharing of contact details of any nature between staff and pupils 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, including Teaching Assistants and Supply Teachers must read and sign the acceptable 'ICT Acceptable User Agreement' before using any school ICT resource.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's 'Acceptable Use Policy'.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

## ASSESSING RISKS

- 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The headteacher will ensure that the e-Safety Policy is implemented and compliant with the policy monitored.

## 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 head teacher.
- 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.
- Sanctions within the school discipline policy will be carried out.

## COMMUNICATIONS POLICY

### INTRODUCING THE E-SAFETY POLICY TO PUPILS

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

### 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.

---

## LINKED POLICIES

Anti-Bullying Policy

Behaviour Policy

Safeguarding & Child Protection Policy

Curriculum Policy

Data Protection Policy

Health & Safety Policy

PSHE Policy

---

DATE PUBLISHED: OCTOBER 2016


REVIEW DATE: OCTOBER 2017

APPROVED BY: ALIMUDDIN SHAIKH (HEADTEACHER)

## 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.	Pupils should be supervised.  Pupils should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	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 Picsearch safesearch <b>NOT Google images</b>
Publishing pupils' work on school and other websites.	Pupils' full names and other personal information should be omitted.	School website
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.	School website

**APPENDIX 2: ACCEPTABLE USE AGREEMENT: ALL STAFF, VOLUNTEERS AND GOVERNORS**

	<b>Name of School</b>	<b>Harrow Primary School</b>
	<b>AUP review Date</b>	<b>September 2015</b>
	<b>Date of next Review</b>	<b>September 2016</b>
	<b>Who reviewed this AUP?</b>	<b>Alimuddin Shaikh (Headteacher)</b>

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Trustees/Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.  
This is currently: name@harrowprimary.org.uk
- I will only use the approved email system and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the appropriate line manager / school named contact – namely, the Headteacher.





- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school's policy on use of mobile phones / devices at school i.e. not use these for photography in classrooms and any such protocols.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- 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 will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using Office365 and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management 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 alert the child protection officer (Alimuiddin Shaikh) or appropriate senior member of staff (Zahra al Hilli) if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the designated Child Protection lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Headteacher / Safeguarding Lead* on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- *Staff that have a teaching role only:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

ACCEPTABLE USE POLICY (AUP): AGREEMENT FORM - ALL STAFF, VOLUNTEERS,  
GOVERNORS

**User Signature**

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date.....

Full Name ..... (printed)

Job title / Role .....

**Authorised Signature (Head Teacher / Deputy)**

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date.....

Full Name ..... (printed)

---



## E-SAFETY AGREEMENT FORM: PARENTS

**Internet and ICT:** As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- ICT facilities and equipment at the school.



I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.



I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.



Use of digital images, photography and video: I understand the school has clear protocols on "The use of digital images and video" and I support this.



I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.



I will not take and then share online, photographs of other children (or staff) at school events without permission.



Social networking and media sites: I understand that the school has a clear No Use (in school) policy for students on "The use of social networking and media sites" and I support this.



I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

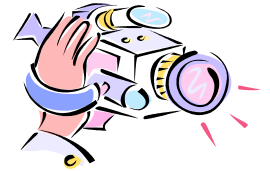


**My daughter / son name(s):** \_\_\_\_\_

**Parent / guardian signature:** \_\_\_\_\_

**Date:** \_\_\_ / \_\_\_ / \_\_\_





## 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 the following rules for any external use of digital images:

**If the pupil is named, we avoid using their photograph.**

**If their photograph is used, we avoid naming the pupil.**

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

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video; pupils' full names aren't given in credits at the end of the film.

Only images of pupils 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.
- 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 CDROM / 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 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

*How do we show common courtesy online?*

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

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

*How do we show common sense online?*

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) 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 network sites, they will be reported to the appropriate 'report abuse' section of the network site.

*(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)*

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:

<https://www.thinkuknow.co.uk/parents/browser-safety/>