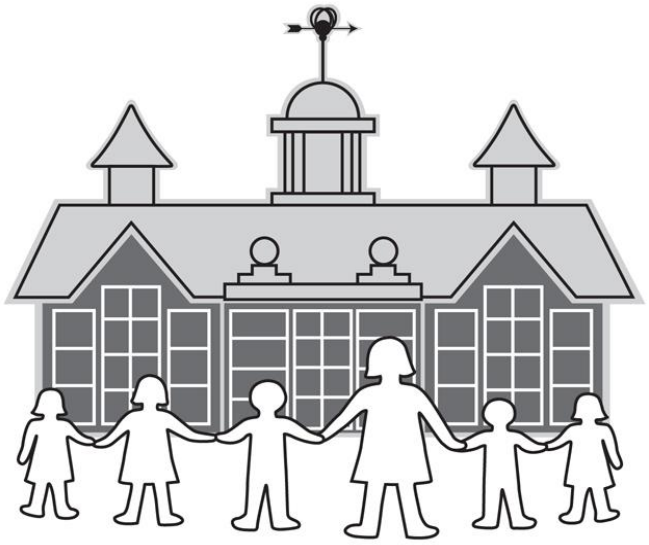
North Ealing Primary School



e-Safety Policy

School lead for this policy: Nic Mehew	
Committee with oversight for this policy - Curriculum & Standards	
Policy to be approved by the Curriculum & Standards Committee	
Policy last reviewed by the Curriculum & Standards Committee	17/06/2015
Policy last ratified and adopted by Full Governing Body	N/A
Policy / Document due for review	06/2018

North Ealing Primary School
e-Safety Policy

Background

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, NES needs to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At North Ealing, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The ICT Coordinator is the eSafety co-ordinator at North Ealing. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Ealing LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying and PHSE policies.

eSafety skills development for staff

- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Managing the school eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed.
- The school uses eSafety and Security software – Sophos provided by the London Grid for Learning (LGFL). Automatic updates provides security for the whole network and teachers laptops.
- LGFL Staffmail, which is a secure, high specification email service using Microsoft Exchange, is used by all staff.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school provides opportunities within a range of curriculum areas to teach about eSafety. At Meet the Parents evening, parents are reminded of the importance of safety at home. Children are taught to surf the Internet safely

when doing research. "Think U Know" DVD is used to remind children of how to keep safe on line. Digismart Computer Club has several sessions on esafety and their posters are displayed throughout the school.

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as ChildLine/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum *i.e. Year 5 QCA unit 5c Evaluating Information, Digismart activities.*

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read *and sign* an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Staff are provided with an individual network, email and Learning Platform log-in username. From *Year 1* pupils are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If pupils think their password may have been compromised or someone else has become aware of their password they must report this to the teacher who will then inform the ICT Coordinator.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the HT
- Any data taken off the school premises must be encrypted.

- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any *school/ children/ pupil* data

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- Ealing Local Authority has a monitoring solution via the London Grid for Learning. Upon request, web-based activity can be monitored and recorded.
- School internet access is controlled through the LGfL's web filtering service.
- North Ealing is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
- Sophos Anti-Virus protection is provided by the LGfL and is set to automatically update on all school machines. This is the responsibility of *Yosabe our technical support company.* In addition staff laptops used at home are protected by Sophos Anti-Virus as agreed by the LGfL.
- Staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT Coordinator.
- If there are any issues related to viruses or anti-virus software, the *technical support company* should be informed by recording in the ICT log book.

Personal Mobile devices

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.

- Pupils are allowed to bring personal mobile phones to school and must be handed into the office on arrival and collected at the end of the day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Capturing images & video is not allowed by students / staff unless on school equipment and for educational purposes.

Managing email

- The school gives all staff their own LGfL StaffMail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Staff must inform the ICT Coordinator if they receive an offensive e-mail
- Pupils at North Ealing are not given access to email accounts.

Safe Use of Images / Film - Taking of Images and Film

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the schools network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the schools network and deleted from the pupils device.
- Images of pupils are deleted when pupils leave the school.

Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform / MLE.

Complaints

Complaints relating to eSafety should be made to the ICT Coordinator or Headteacher. Incidents should be logged and process should be followed .

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

Acceptable Use Agreement: Staff, Governors and Visitors
Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with NAME, NES eSafety coordinator.

- I will only use the school's email / Internet / MLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role, and never via personal email / phone.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) and MLE tools for communications with pupils / students / parents.
- I am aware that communicating with students / pupils via private email / SMS/Facebook and social networking sites may be considered a disciplinary matter in this school.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of XXX
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- **Understand that to do so may constitute a disciplinary offence and in some cases a criminal offence.**
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will not communicate with any pupil via email or networking site e.g. Facebook.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….…… Date ……

Full Name …….....(printed)

Job title . . . . . .

Pupil Acceptable Use
Agreement / eSafety Rules

I will only use ICT in school for school purposes.
I will only open email attachments from people I know, or who my teacher has approved.
I will not tell other people my ICT passwords OR use any one else's.
I will only open/delete my own files.
I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
I will not give private details (home address, mobile number, email address etc) to people I meet online.

Dear Parent/ Carer

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact ***the ICT Coordinator***.

✂- -

Parent/ carer signature
We have discussed this and ……………………………………..........(child name) agrees to follow the eSafety rules and to support the safe use of ICT at North Ealing School.

Parent/ Carer Signature ……..…………………..…………………………….

Class …………………………………. Date ………………………………