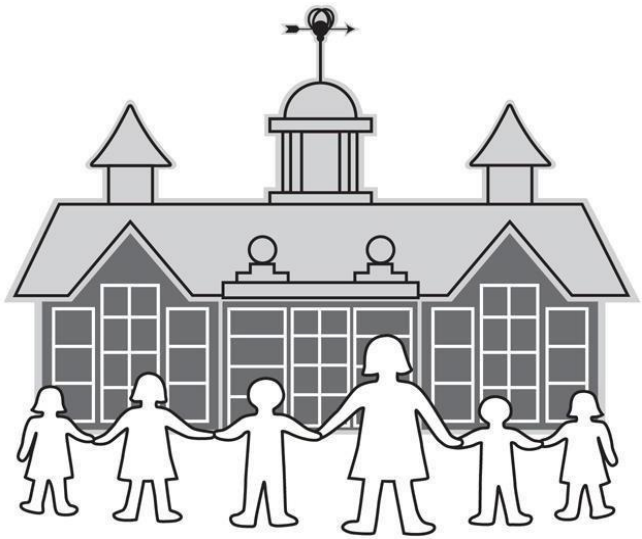
North Ealing Primary School



Online Safety Policy

School lead for this policy: Nic Mehew	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	20/06/2018
Policy last ratified and adopted by Full Governing Body	N/A
Policy / Document due for review	June 2021

Policies that should be read in conjunction with this policy are as follow:

- **Anti Bullying**
- **Child Protection policy**
- **Data Protection**
- **Freedom of Information**
- **Health & Safety**
- **History**
- **Home / School Agreement**
- **ICT / Computing**
- **PSHE Policy**
- **Safeguarding Statement**
- **Whistleblowing Policy**

Key Sites that inform/supplement/deliver this policy:

- **https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis**
- **https://www.lgfl.net/online-safety/resource-centre?s=24**
- **https://swgfl.org.uk/products-services/online-safety/**
- **https://www.lgfl.net/online-safety/**
- **http://neslearningzone.com/esafety/**

North Ealing Primary School
Online Safety Policy 2019-2020

Background

ICT in the 21st Century 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 and social media,, 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 about online safety issues as part of our safeguarding responsibilities.; teaching them the appropriate behaviours and critical-thinking skills that 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).

The changes to data-protection introduced May. 2018, require that ALL of the school community accepts and adopts the role of 'safe-guarder' and accepts/adapts to the need for absolute commitment to the aims of the GDPR initiative – knowing that infringement of its requirements has far-reaching consequences to individuals, the school, the community and possible fines!

Roles and Responsibilities:

Online safety is a key component of strategic leadership within the school: the Head and governors have ultimate responsibility to ensure that the policy and practices outlined in this policy are embedded and monitored. The ICT Coordinator is also the online-safety co-ordinator at North Ealing although ALL staff must assume responsibility and observe due diligence both personally and for their pupils. All members of the school community have been made aware of who holds this post. It is the role of the online safety 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. S/he is also included in the Safeguarding Group and meets regularly if the Safeguarding lead/governor and pupil representatives.

Senior Management and Governors are updated by the Head/ online safety co-ordinator and all governors must 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: Safeguarding child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying and PSHE policies.

Online safety skills development for staff:

- New staff must 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 online safety and know what to do in the event of misuse of technology by any member of the school community –to inform the lead who will decide upon the best course of action.
- All staff are required to incorporate online safety activities and awareness within their curriculum areas. There is an online safety curriculum on Central Resources for reference and these are also built in to the new Computing Curriculum for 2018-19.

Acceptable Use Policies (AUP)

For full details, see Appendix A.

- NES updates its AUPs every year due to the ongoing development of technological advance.
- NES applies an AUP for Staff (all, not just teachers), Pupils (General and specifically for Early Years) and Visitors.
- As NES is now a paperless school, the AUPs are published clearly on the school website. All members of the staff community are made aware of this and requested to digitally-sign using school comms .Parents are made aware at the 'Meet the Teacher' evening in September of each new academic year. Staff are made aware in Staff Meetings and when joining the school. FAILURE TO DIGITALLY-SIGN IS NOT AN EXEMPTION FROM THE EXPECTATIONS. It is the personal responsibility of staff, pupils, parent/guardians/ visitors to read and apply the expectations outlined in the appropriate AUP.

Managing the school online safety messages:

- We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used through reminding pupils of how to use the 'panic buttons' installed on all devices and reminders about how to search effectively.
- The online-safety policy will be introduced to the pupils at the start of each school year at age-appropriate levels.
- Online safety posters will be prominently displayed throughout the school.
- The school uses Online safety and Security software – Sophos provided by the London Grid for Learning (LGFL). Automatic updates provide 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.

Online safety in the Curriculum:

Computing and online resources are essential elements of the whole curriculum. We believe that it is essential fo guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum , directly and discretely: we continually look for new opportunities to promote digital literacy.

- The school provides opportunities within a range of curriculum areas to teach about online safety. At 'Meet the Parents' evening, parents are reminded of the importance of safety at home.
- The NES Learning Zone has a comprehensive and regularly-updated resource bank that inform parents of the latest apps/ social media issues.
- Educating pupils on the dangers of technologies/apps that may be encountered outside of school is delivered informally when opportunities arise and as part of the online safety 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. They need to understand WHY and the possible effects of accessing

apps whilst underage. The curriculum includes clear modules of guidance (Cyberpass/ Trust Me/ Play,Like,Share) to deliver a consistent and progressive message.

- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities. They are taught to 'decode' 'terms and conditions' so that they understand what they are signing up to.

- Pupils know about 'fake news' and are taught how to identify this; they know that not everything they see online is 'true'.
- Pupils are made 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 search skills through cross curricular teachermodellling, discussions and via the Computing curriculum

APPENDIX A includes the current online safety curriculum but new resources are introduced as and when they are made available.

Password Security:

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff members 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. For example, the co-ordinator will ask to check phones by asking for passwords in an informal environment. Pupils need to understand that they must question motives even from a trusted adult.

- The school community – staff, parents, pupils, visitors – are expected to agree to the appropriate Acceptable Use (AU) policy. These are online on the school's main website. Being paperless, requires that agreement is ensured via school comms. It is the responsibility of the individual todigitally-sign acceptance. Failure to do so DOES NOT exempt them from adherence to our requirements.

- Staff members are provided with an individual network, email and LGfL platform password. 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 orothers unless led by the responsible teacher.

- If pupils think their password may have been compromised or someone else has become aware of their password they must report this to their teacher who will then inform the Computing/Online safety co-ordinator.

Data Security:

The accessing and appropriate use of school data is something that the school takes very seriously. The introduction of GDPR (May 2018) will impact significantly on how the school community adjusts and accommodates its very specific requirements:

- Staff members must be made aware of their responsibility when accessing school data. Level of access is determined by the Headteacher.
- Any data taken off the school premises must be encrypted and secured if on paper ie use of Datasur keys.
- 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 that 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/videos/links/resources before use.
- Raw image searches are unacceptable when working with pupils.
- Our YOUTUBE settings are set at 'moderate' but materials MUST BE VIEWED IN FULL prior to display and links on the 'suggestions' panel must be looked at to check for appropriateness.
- The use of 'my videos' on my.uso.im is the best way forward although content is limited. Staff members must check accessibility in school.
- 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.

- Use of the NES Learning Zone or my.uso.im is advised due to the controls in place.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

Infrastructure:

- Ealing Local Authority has a monitoring solution via the London Grid for Learning. Upon request, web-based activity can be monitored and recorded. The latest 'mystats' tool is being trialled at North Ealing to assist in this process.
- 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, GDPR May 2018.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- Staff and pupils are aware that blogs sent to NES Learning Zone are MODERATED and that iep addresses are displayed to the moderator.
- If staff or pupils encounter an unsuitable site, the screen must be switched off/ closed via the alarm button and the incident reported immediately to the online 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 members are not permitted to download programs or files on school- based equipment without seeking prior permission from the Computing Coordinator.
- If there are any issues related to viruses or anti-virus software, the YOSABE or the co-ordinator should be informed by recording in the 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 UNLESS the need is that of safeguarding or an emergency.

- Pupils are allowed to bring personal mobile phones to school but these must be handed into the office on arrival and collected at the end of the day. They must also be clearly-named.
- 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 (see Whistleblowing Policy)
- 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 for educational purposes.
- The school provides image-capturing devices and these are to be used whenever possible/practical.

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 their 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. Currently, some year groups are using DOJO contacts – this will be reviewed after May 25th 2018.
- Staff must inform the Coordinator if they receive an offensive e-mail or inappropriate spam mail.
- Pupils at North Ealing are not given access to LGfL email accounts.

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

- With the consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Parents can elect to have NO images taken, only images used in school or general permission.
- Parents are advised and requested to NOT share images/videos of assemblies/ concerts etc on social media (eg Youtube) as this is an infringement of the rights of others.
- 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.

- **Pupils are not permitted to use personal digital equipment/ mobile phones, to record images of others - disposable cameras are a possible exemption.**
  - Images of pupils must be 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.
- All staff must know the pupils that CANNOT have their image taken/used without the express, possibly exceptional, permission of their parent/guardian.

Complaints:

Complaints relating to online safety issues should be made to the Coordinator or Headteacher as soon as possible. Incidents should be logged
All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Coordinator.

- Deliberate accessing of inappropriate materials by any staff user will lead to the incident being logged by the 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

Appendix A: Current Online Safety Curriculum:

Progression of online safety Resources 2019-2020 - KS1 & KS2

The new Ofsted handbook and guidance have made the expectations that need to be met very clear. This is a summary of them:

• All teaching and non-teaching staff should be aware and able to recognise online-safety issues with high-quality leadership and management to make online-safety a priority
• High priority given to training and continuation training to all staff, including the contribution of the wider school community. One member of staff to receive accredited training (for example: to become an online-safety officer)
• Clear reporting processes
• Rigorous, plain English policies and procedures integrated with other relevant policies
• Progressive online-safety curriculum
• Provision of a recognised internet service provider (ISP) with age-related filtering
• Good risk assessment

Our online safety curriculum is taught throughout the year in assemblies, special events (Safer Internet Day in February) and as part of Computing/PSHE.

Our ONLINE SAFETY CURRICULUM supports the UNICEF Rights of the Child Agenda:

- Article 15 You have the right to choose your own friends and join or set up groups, as long as it isn't harmful to others.
- Article 16 You have the right to privacy.
- Article 17 You have the right to get information that is important to your well-being, from radio, newspaper, books, computers and other sources. Adults should make sure that the information you are getting is not harmful, and help you find and understand the information you need.
- Article 13 You have the right to find out things and share what you think with others, by talking, drawing, writing or in any other way unless it harms or offends other people.
- Article 36 You have the right to protection from any kind of exploitation

Online Safety Resources

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
	Timetabled Events:		**Timetabled Events:**		**Timetabled Events:**	
	<u>We will find a new 'NESSIE' (North Ealing School's Safer Internet Environment mascot!).</u> • **September 'Nessie'** • **February SID (Safer Internet Day)** • **https://www.saferinternetday.org/**		**<u>We will find a new 'NESSIE' (North Ealing School's Safer Internet Environment mascot!).</u>** • **September 'Nessie'** • **February SID (Safer Internet Day)** • **https://www.saferinternetday.org/**		**<u>We will find a new 'NESSIE' (North Ealing School's Safer Internet Environment mascot!).</u>** • **September 'Nessie'** • **February SID(Safer Internet Day)** • **https://www.saferinternetday.org/**	
Autumn	***<u>will discuss the differences between real / online friends.</u>*** • General discussion around friendship – how do you KNOW who is a friend? • When online, do we KNOW if they are who they say they are • When do we FEEL that something is not right and what should we do?		***<u>We will review the Nessie Code of Conduct and explore out lives in the web.</u>*** • Include section about online safety in Class Code of Conduct. • Display 'Nessie' entries. Year 3 'Play, Like and Share' • https://www.thinkuknow.co.uk/4_7/child/ • Plus use of associated game: 'Band Runner'. • https://www.thinkuknow.co.uk/8_10/ Year 4: Revisit 'Band Runner' game.		***<u>We will review the Code of Conduct and engage in discussion using CYBERPASS.</u>*** • CYBERPASS ongoing. • TEACHER LINK GUIDE: • https://videocentralhd.lgfl.org.uk/premium_play.aspx?id=dJvtJa7yNtGZwp • <u>Pupil</u> link on YEAR 6 my.uso.im page. • Years 5/6 to negotiate access. Suggest watching the case study video first.	

	Spring	**Year 1 & 2** ***We will take part in the SID assembly and follow up using the resources provided.*** • Use of the Safer Internet Day (SID) resources to complement the SID Assemblies in February. Preparation and Consolidation. **Year 1:** ***We will learn about how to be RESPONSIBLE and SENSITIVE on line.*** • https://www.childnet.com/resources/digiduck-stories/digiducks-big-decision • Images and 'fake news'. Video Book. **Year 2:** ***We will learn how to THINK about people online and make sensible decisions. We understand who deserves to be a 'celebrity' or not!*** https://www.childnet.com/resources/digiduck-stories/digiducks-famous-friend Who to believe online? Video book.	**Year 3 & 4:** ***We will take part in the SID assembly and follow up using the resources provided.*** • Use of the Safer Internet Day (SID) resources to complement the SID Assemblies in February. Preparation and Consolidation. **Year 3:** ***We will explore our online lives and lean about the pros and cons!*** • Us Online – interactive unit from LGfL on my.uso.im LOG-IN required **Year 4:** (you need to order resource pack in advance). ***We will learn how to become RESPONSIBLE in our online lives.*** • https://parentzone.org.uk/be-internet-legends ***We will learn how develop our critical thinking skills!*** • Advertising/fake news/ critical thinking: • https://mediasmart.uk.com/an-introduction-to-advertising-for-7-11-yrs/	**Year 5 & 6:** ***We will take part in the SID assembly and follow up using the resources provided.*** • **Cyberpass ongoing.** • Use of the Safer Internet Day (SID) resources to complement the SID Assemblies in February. Preparation and Consolidation. **Year 5**: 'Trust Me' – critical thinking with resources. ***We will learn about CRITICAL THINKING and how to avoid problems online!*** • https://www.childnet.com/resources/trust-me • **Year 5/6**: Mental Health /online manipulation/ critical thinking: • https://mediasmart.uk.com/body-image-9-11/

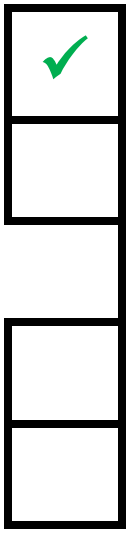
	Summer	***We will learn how to be safe online and be good digital citizens.*** • EYFS/Years ½:'Smartie the Penguin' sequence for each year group with resources. • https://www.childnet.com/resources/smartie-the-penguin	**Year 3:** • Sharp/Alert/Secure/Kind/Brave – to download. • https://parentzone.org.uk/be-internet-legends **Year 4:** ***We will review our understanding of online safety.*** • https://www.saferinternet.org.uk/safer-internet-day/2018/digital-friendships-quiz • 10 questions to share/discuss in class after interactive participation.	**Year 5:** ***We will learn about how to 'spot' potential dangers online.*** • Show 'Jigsaw' /discussion/ SRE/ Critical Thinking • https://dotsub.com/view/31a6df22-6e22-4558-90d1-3a366c5cbaf8 **Year 6:** ***We will learn about how things can 'change' as we move on.*** • Show 'Consequences' – sensitive material so preview! • https://assemblytube.com/forum/key-stage-3-video-assemblies/internet-safety-consequences-ceops-assembly/ • OR: • https://www.bbc.co.uk/newsround/13908828

Appendix B: AU Agreements

https://static.lgfl.net/LgflNet/downloads/online-safety/LGfL-OS-AUP-Pupil-KS1-2017.docx

Key Stage 1: Acceptable Use Agreement North Ealing Primary School 2019-20

This is how I keep **SAFE online**:



1. I only use the devices I'm **ALLOWED** to
2. I **CHECK** before I use new sites, games or apps
3. I **ASK** for help if I'm stuck
4. I **THINK** before I click

5. I **KNOW** people online aren't always who they say

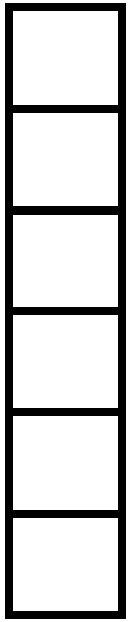
6. I don't keep ~~**SECRETS**~~ just because someone asks me to

7. I don't change **CLOTHES** in front of a camera

8. I am **RESPONSIBLE** so never share private information

9. I am **KIND** and polite to everyone

10. I **TELL** a trusted adult if I'm worried, scared or just not sure



My trusted adults are_____at school

_____at home and _____

https://static.lgfl.net/LgflNet/downloads/online-safety/LGfL-OS-AUP-Pupil-KS2-2017.docx

KS2 Pupil Online Acceptable Use Agreement 2019-20

This agreement will help keep me safe and help me to be fair to others

- ***I am an online digital learner*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.

- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, gams and apps that my trusted adults have agreed to.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.
- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.

- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

https://static.lgfl.net/LgflNet/downloads/online-safety/LGfL-OS-AUP-Staff-Volunteers-Contractors-2017.docx

School logo	Name of School	North Ealing Primary
	AUP review Date	June 2018
	Date of next Review	June 2019
	Who reviewed this AUP?	Nic Mehew

Acceptable Use Agreement: Staff, Volunteers, Governors & Contractors 2019-20

What is an AUP?

We ask all children, young people and adults involved in the life of North Ealing Primary School to agree to an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy which can be viewed on the School Website www.northealingprimary.org

Where can I find out more?

All staff, governors and volunteers should read North Ealing Primary School's full Online Safety Policy on the school's website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to M.Belsito (Deputy Head/Safeguarding Lead or N.Mehew (Online Safety lead) admin@northealing.ealing.sch.uk

What am I agreeing to?

1. I have read and understood North Ealing Primary School's full Online Safety policy via http://northealingprimary.org/information/school-policies-2.html and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (M.Belsito/N.Mehew)
3. I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.
4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy http://northealingprimary.org/policies/ma.%20online%20Safety.pdf I will report any breach of this by others or attempts by pupils to do the same.
7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
8. I understand the importance of upholding my online reputation, that of the school and of the teaching profession), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in North Ealing Primary's School social media policy/guidance.
9. I understand that school systems and users are protected by security, monitoring and filtering services, so my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/or relevant/authorised staff members.
10. I agree to adhere to all provisions of the school Data Protection Policy http://northealingprimary.org/policies/GDPR%20-%20Data%20Protection%20Policy%20November%202018.pdf at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify M.Belsito or N.Mehew. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times. All school data MUST be encrypted using the provided datakeys (DataSur)
11. I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring, will look after devices loaned to me, and will notify the school of "significant personal use" as defined by HM Revenue & Customs.
12. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

http://northealingprimary.org/policies/North%20Ealing%20Primary%20School%20Safeguarding%20Statement.pdf

13. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
14. I will follow the guidance in the Online Safety Policy for reporting incidents but also any concerns I might think are important – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture, but only if I tell somebody. I have read the sections on handing incidents and concerns about a child in general, sexting, bullying, sexual violence and harassment, misuse of technology and social media.
15. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

PLEASE ENSURE THAT YOU SIGN AND DATE THE REGISTER AS EARLY AS POSSIBLE IN THE SCHOOL YEAR.

FAILURE TO DO SO DOES NOT EXEMPT YOU FROM THE REQUIREMENTS OF THE AU.