North Ealing Primary School

Online 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	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 2018-2020

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 teacher modellling, 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.

<u>Password Security:</u>

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 or others 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 xxxx-xxxx

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

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
	Timetabled Events:		**Timetabled Events:**		**Timetabled Events:**	

	September 'Nessie' **February SID (Safer Internet Day)** **https://www.saferinternetday.org/** **FREQUENT input throughout year in class.**	**September 'Nessie'** **February SID (Safer Internet Day)** **https://www.saferinternetday.org/** **FREQUENT input throughout year in class.**	**September 'Nessie'** **February SID(Safer Internet Day)** **https://www.saferinternetday.org/** **FREQUENT input throughout year in class.**
	Hector's World (5 online videos) www.thinkuknow.co.uk	**Dongle the Rabbit** & BBC "Safesurfing" website www.bbc.co.uk/cbbc/help/web/staysafe **'Play, Like and Share'** **https://www.thinkuknow.co.uk/** **(NEW NOVEMEBER 2016!)**	**CYBERPASS ongoing.** **TEACHER LINK GUIDE:** **https://videocentralhd.lgfl.org.uk/premium_play.aspx?id=dJvtJa7yNtGZwp** **https://content.lgfl.org.uk/secure/cyberpass/cyberpass/quizzes**
	CEOP: Lee & Kim's Animal Magic Adventure (video & song) www.thinkuknow.co.uk	**CEOP: "Josh & Sue are Friends"** www.thinkuknow.co.uk **CyberCafe** https://www.thinkuknow.co.uk/8_10/	**CEOP video – "Becky"** www.thinkuknow.co.uk

		ChildNet: "Captain Kara & Winston's SMART Adventures" www.childnet-int.org.uk/kia/primary	**LGfL "Us Online"** (needs individual USO log-in) www.usonline.lgfl.net
			'TRUST ME' (Content/Contact unit 'assess digital content) **https://www.lgfl.net/online-safety/trust-me**

There are other CEOP videos aimed at the 11 - 14 age range. **"Let's Fight it Together"** ~ A boy is relentlessly teased and bullied by phone text and internet.

"Consequences" ~ an older teenage boy harvests online information to befriend a teenage girl. He coaxes & extorts her to provide increasingly sexual images. USE WITH CAUTION!

"Exposure" ~ a teenage girl regrets sending her boyfriend a few saucy photos through her phone as he shares them with all the world.

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 2017-18

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

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.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Signed: ______________________________ Date: ______________

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

Covers use of all digital technologies while in school: i.e. **email, internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, apps **and other relevant digital systems provided by the school or school umbrella body (Local Authority, Academy, Free School Trust, etc).**

Also covers school equipment when used outside of school, use of online systems provided by the school or school umbrella body when accessed from outside school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.

North Ealing Primary regularly reviews and updates all AUP documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and 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 and change my passwords regularly. 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 / social networks / mobile apps / or any other system I have access to via the school or school umbrella.
- 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 LGFL Staff Mail
- I will only use the approved method/s of communicating with pupils or parents/carers and only communicate with them in a professional manner and on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- 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 [ICT co-ordinator0
- 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 connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.

- 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 or on any personal devices.
- I will follow the school's policy on use of mobile phones / devices at school
- 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 only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.
- I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.
- 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 the *LGfL / school approved system* 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 am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.
- 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 relevant Senior Member of Staff / Designated Safeguarding Lead [Michael Belsito)
- I understand that all internet and network traffic / usage can be logged and this information can be made available *to the Head* / *Safeguarding Lead* on their request.
- I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
- *Staff that have a teaching role only:* I will embed the school's online 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 online safety / safeguarding 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)