



**1.21 Online safety
and IT Use Policy
(EYFS & KS1-3)**

Reviewer responsible:	DSL and Head of Digital Learning	Date of last review:	08/26
Reviewed by:	JH/LK	Date of next review:	05/27
Authorised by:	Exec		

Notting Hill Prep School, 95 Lancaster Road, London W11 1QQ
020 7221 0727 admin@nottinghillprep.com
nottinghillprep.com

Notting Hill Preparatory School Ltd. is a company registered in England and Wales. Company no. 04677024

Introduction

Notting Hill Preparatory School recognises that digital technology is an integral part of teaching, learning, communication and school operations. Technology provides significant educational opportunities, supporting creativity, collaboration, digital literacy and access to information, while also presenting safeguarding, cybersecurity and data protection risks that must be managed carefully.

This policy sets out the school's expectations for the safe, responsible and effective use of technology and digital systems by pupils, staff, governors, visitors and the wider school community. It outlines the measures in place to safeguard pupils and staff, protect school systems and data, and promote positive digital behaviour both in school and when working remotely.

The school is committed to maintaining a culture of online safety, digital responsibility and cybersecurity awareness through education, monitoring, appropriate technical controls and clear reporting procedures. Any breach of this policy may result in safeguarding action, withdrawal of IT access, disciplinary procedures and/or referral to external agencies where appropriate.

1. Aims

In accordance with the school's safeguarding responsibilities, the **Education Act 2002** and **Keeping Children Safe in Education (KCSIE)**, this policy aims to:

- safeguard and protect pupils, staff and the wider school community when using technology and online platforms;
- promote the safe, responsible and effective use of digital technology across the school;
- support pupils in developing the knowledge, skills and critical understanding needed to stay safe online and become responsible digital citizens;
- establish clear expectations for the acceptable use of school systems, devices, communication platforms and online services;
- support staff in using technology safely, professionally and confidently, including through training in digital literacy, cybersecurity and artificial intelligence;
- protect the confidentiality, integrity and security of school systems, devices and data;
- ensure appropriate filtering, monitoring and safeguarding procedures are in place and understood by staff;
- promote a culture of reporting, accountability and responsible digital behaviour;
- minimise the risk of harm, safeguarding incidents, data breaches or misuse of technology;
- ensure that unlawful, unsafe or inappropriate behaviour involving technology is addressed appropriately in line with school policies and procedures.

2. Roles and responsibilities

Online safety and digital safeguarding are the responsibility of the whole school community. All members of the community have a role in ensuring that technology is used safely, responsibly and effectively to support learning and wellbeing.

Senior Leadership

- The DSL is the designated senior leader responsible for the school's filtering and monitoring arrangements. They will work with the Heads of Digital Learning and technical staff to ensure that filtering and monitoring systems are appropriate, effective and reviewed regularly.
- The DSL holds overall responsibility for online safety and digital safeguarding provision across the school, supported by HoDL, DDSLs, the Head and SLT.
- The DSL will oversee the implementation, review and day-to-day management of online safety procedures and incident response.
- Safeguarding concerns relating to technology or online activity will be managed in accordance with this policy and the Safeguarding and Child Protection Policy.
- Appropriate staff training and updates relating to online safety, filtering and monitoring will be provided regularly.
- Online searches of shortlisted candidates may be carried out as part of safer recruitment procedures.

Head of Computing and Head of Digital Learning

- To promote and support a strong culture of online safety across the school.
- To support the DSL and DDSLs in the implementation and review of online safety procedures.
- To liaise with technical staff and senior leaders regarding filtering, monitoring and online safety matters.
- To support the delivery of digital literacy and online safety education across the curriculum.
- To support staff and parents in understanding current online safety risks, trends and safe use of technology.
- To oversee the use of classroom.cloud and other monitoring systems used within the school.

Classroom Teachers and Support Staff

- To read, understand and follow the school's online safety policies and Acceptable Use Agreements.
- To model safe, responsible and professional use of technology at all times.
- To use only school-approved communication systems when communicating with pupils or parents.
- To supervise and guide pupils appropriately when using technology for learning.
- To reinforce online safety and digital literacy messages through teaching and daily practice.
- To report safeguarding, filtering, monitoring or cybersecurity concerns promptly through the school's reporting procedures.

- To maintain appropriate professional conduct online and manage their own online reputation responsibly.
- To use classroom.cloud and other classroom monitoring tools appropriately to support safeguarding and classroom management.

Technical Staff

- To support the school in maintaining secure and reliable IT systems and infrastructure.
- To maintain filtering, monitoring, security and access controls across school systems and devices.
- To report safeguarding or cybersecurity concerns promptly to the DSL or appropriate member of staff.
- To ensure that systems, software, backups and security protections are appropriately maintained and updated.
- To support the school in responding to incidents relating to safeguarding, security or misuse of technology.

Governing Body

- The governing body will ensure that appropriate filtering and monitoring systems are in place, that their effectiveness is reviewed at least annually, and that appropriate oversight and assurance is provided in relation to online safety, safeguarding and digital risk.

3. Managing Digital Content

The use of images, video, audio and online content can enrich teaching and learning, but must be managed carefully to safeguard pupils and staff. Pupils should be taught to use digital content responsibly and understand how to share and manage content safely online.

Consent and Publication

Written parental consent will be obtained before photographs or videos of pupils are published. Consent forms part of the home-school agreement and may be withdrawn in writing at any time.

Images or video may be used:

- on the school website or online platforms;
- on the school's official social media channels;
- in school publications, promotional material or displays;
- in educational presentations or conferences.

Use of Images, Video and Audio

- Staff and pupils should use digital content responsibly and appropriately at all times.
- Pupils will be reminded about the risks associated with sharing images, video and audio online.
- School equipment should normally be used to create or store images, video or

audio relating to school activities.

- Images and recordings should only be taken with appropriate permission and should reflect suitable educational activities.
- Full names of pupils will not be used alongside images or recordings published online.
- Pupils will be taught about copyright, ownership and responsible use of digital media.

Use of Personal Devices

In exceptional circumstances, personal devices may be used for school-related images or recordings with permission from a member of SLT and following completion of a risk assessment (Appendix 1).

Where personal devices are authorised:

- all content must be transferred securely to a school device or system as soon as possible;
- content must be deleted promptly from the personal device once transferred;
- personal devices must not be used to store pupil images or recordings long-term.

Parents and Visitors

Parents and visitors may take photographs at school events for personal use only. Images or videos containing children other than their own should not be shared publicly or uploaded to social media without permission.

Remote Learning

Where remote learning is used, online lessons for Years 5–8 will be delivered through Microsoft Teams using school-approved accounts and security settings. Staff and pupils are expected to follow the Acceptable Use Agreements at all times.

4. Staff training

Staff will receive regular training and updates relating to online safety, safeguarding, filtering, monitoring and the safe use of technology.

As part of induction, all new staff will receive guidance on the school's Online safety Policy, Acceptable Use Agreements and their responsibilities relating to safeguarding and the use of technology.

Staff will be made aware of reporting procedures relating to safeguarding, cybersecurity and misuse of technology, and will be encouraged to promote digital literacy and online safety through their teaching and wider interactions with pupils.

Staff will also receive training to support their own digital literacy and professional use of technology, including the safe, effective and responsible use of artificial intelligence

tools.

5. Passwords

Passwords are an important part of keeping school systems and information secure. All staff and pupils are responsible for maintaining the security of their accounts and login details.

- Secure username and password systems are used for access to school IT systems, including email, network access and school platforms.
- All pupils and staff will have individual user accounts. Password complexity will increase appropriately with age and level of system access.
- Passwords must not be shared or used by anyone other than the authorised account holder. Users must not attempt to access accounts, systems or data which they are not authorised to use.
- Any suspected compromise of account security must be reported promptly and passwords changed immediately.
- Staff and pupils will be reminded regularly about safe password practices and the importance of keeping login details secure.
- All staff will read and sign the Staff Acceptable Use Agreement (Addendum 1) before accessing school systems. Pupils in Key Stage 2 and 3 will sign the Pupil Acceptable Use Agreement (Addendum 2) annually. In Key Stage 1, teachers will explain the agreement in an age-appropriate way and sign on behalf of the class.

6. Filtering Internet Access

The school provides filtered internet access to support teaching, learning and school operations while helping to safeguard pupils and staff from inappropriate or harmful content.

Filtering and monitoring systems are provided through LGfL and are reviewed regularly to ensure they remain appropriate to the age and needs of pupils.

The school will take reasonable steps to restrict access to illegal, inappropriate or harmful material, while recognising that no filtering system can be completely effective.

Any concerns relating to inappropriate content, filtering breaches or online safety incidents must be reported promptly to the DSL, Heads of Digital Learning or an appropriate member of staff. Relevant incidents may be recorded on CPOMS and reviewed as part of the school's safeguarding and monitoring procedures.

Filtering, monitoring and block lists may be reviewed and amended where appropriate to support safeguarding and educational needs.

7. Acceptable and Prohibited Use of School IT Systems

Staff must not:

- access, create, store or share illegal, extremist, discriminatory, pornographic or otherwise inappropriate material;
- use school systems to bully, harass or intimidate others;
- attempt to bypass filtering, monitoring or security systems;
- gain or attempt to gain unauthorised access to systems or data;
- intentionally damage school IT systems or data;
- share confidential information without authorisation;
- use inappropriate or offensive language on school communication platforms;
- engage in conduct which may bring the school into disrepute;
- breach copyright, intellectual property or data protection requirements.

Any breach of these expectations may result in safeguarding action, withdrawal of IT access, disciplinary procedures and/or referral to external agencies where appropriate.

8. Use of School Devices and IT Equipment

Staff may be issued with school-owned devices and accessories, including laptops and chargers, to support them in carrying out their role. These remain the property of the school and must be returned upon request or at the end of employment. The school reserves the right to charge for unreturned equipment.

- Staff are expected to use school devices responsibly and exercise reasonable care in their handling, storage and transport.
- Any loss, damage, faults or security concerns should be reported promptly to the Digital Learning team or IT support staff.
- Staff should not install unauthorised software, applications or hardware onto school devices or systems without permission from the Digital Learning team or IT support staff.
- Devices and user accounts should be locked or logged out when left unattended.
- School devices should be stored securely when not in use and must not be left unattended in unsecured areas.
- Staff remain responsible for the secure handling of school devices, systems and data when working offsite or remotely.

The school remains responsible for the management, maintenance, monitoring and security configuration of school-owned devices and systems. Staff should seek guidance or training before using unfamiliar systems or technologies.

9. Cybersecurity

The school takes reasonable steps to protect its systems, devices and data from

cybersecurity threats and unauthorised access. All members of the school community have a responsibility to use technology safely and securely.

- Staff must not install unauthorised software or applications onto school devices or systems without permission from the Digital Learning team or IT support staff.
- Staff should exercise caution when opening attachments, downloading files or accessing links from unknown or untrusted sources. Any suspected malware, phishing attempt or cybersecurity concern should be reported promptly.
- Any personal device used to access school systems or data must have appropriate security and password protection in place.
- Staff must not enter into contracts, subscriptions or software agreements on behalf of the school without appropriate authorisation.
- Staff will receive regular cybersecurity training and updates, including phishing awareness and safe digital practices. Completion of required cybersecurity training is mandatory for all staff.

10. Email Procedures (see also Social Media Policy)

- Staff must use school-provided email accounts and communication platforms for all school-related communication with pupils, parents, carers and external agencies. Personal email accounts must not be used for school business.
- School email accounts and school systems and platforms must be used professionally and in accordance with the school's safeguarding, behaviour, equal opportunities and data protection expectations.
- Staff should be aware that emails and digital communications may be monitored and may be disclosed as part of legal proceedings, safeguarding investigations or subject access requests.
- When communicating with groups of parents or carers by email, addresses should be blind copied (BCC) where appropriate.

11. Mobile Phones

Mobile phones and personal devices must be used responsibly and professionally within the school environment.

- Staff-owned mobile phones and personal devices should not be used during lessons or formal school activities unless permission has been granted in exceptional circumstances or where required for school-related purposes such as multi-factor authentication for systems including CPOMS, iSAMS or Microsoft 365. Devices should normally remain on silent during the school day.
- Personal devices must not be used to photograph, record or store images, video or audio of pupils unless explicitly authorised in line with this policy and supported by an appropriate risk assessment where necessary.
- Staff must not use personal devices or accounts to communicate with pupils or

parents for school-related purposes.

- Mobile phones and personal devices brought into school remain the responsibility of the owner. The school accepts no responsibility for loss, theft or damage.
- Visitors may be provided with access to guest Wi-Fi where appropriate and in accordance with the school's acceptable use expectations.
- Pupils must not have access to or use mobile phones during the school day, including during lessons, transitions, breaktimes and lunchtimes, except where an agreed individual exemption applies.
- Pupils who bring mobile phones to school must hand them in at the beginning of the school day in accordance with school procedures.
- Any misuse of mobile phones or personal devices by pupils may result in confiscation and further sanctions in line with the school's behaviour policies.

12. Data Protection and Information Security

The school holds sensitive and personal information relating to pupils, families and staff. All members of the school community have a responsibility to handle this information securely and appropriately in accordance with data protection legislation and school policies. **(For further details see Policy for Data Protection).**

- Personal and sensitive information will be processed and stored in accordance with UK GDPR and the Data Protection Act 2018.
- Access to school systems and sensitive information will be restricted appropriately through secure accounts, passwords and access controls.
- Staff and pupils must take reasonable steps to protect sensitive information, including locking devices when unattended and ensuring information cannot be viewed by unauthorised individuals.
- Personal or sensitive information taken offsite must be stored and transferred securely using school-approved systems or devices.
- Printed documents containing personal or sensitive information must not be left unattended in public or shared areas.
- The school will maintain appropriate technical and organisational measures to reduce the risk of data loss, unauthorised access or cybersecurity breaches.

13. IT Systems and Access

The school will take reasonable steps to ensure that its IT systems, infrastructure and data are secure, reliable and appropriately maintained.

- Access to systems and services will be controlled through secure authentication and appropriate permissions.
- Servers, devices, software and security systems will be maintained and updated appropriately.
- Appropriate backup and recovery procedures will be in place to minimise disruption or data loss.

- Antivirus, filtering and monitoring systems will be used where appropriate to support safeguarding and cybersecurity.

14. Online Safety Risks

In accordance with Keeping Children Safe in Education (KCSIE) 2026, the School recognises that online safety risks are broad and continually evolving and can be categorised into four areas:

- **Content** – being exposed to illegal, inappropriate or harmful content, including sexual or violent material, discriminatory content, self-harm or suicide content, radicalisation and extremism, misinformation, disinformation, conspiracy theories and harmful or inappropriate AI-generated content;
- **Contact** – being subjected to harmful online interaction with other users or technologies, including peer pressure, grooming, exploitation, inappropriate commercial contact and harmful interactions involving generative AI applications;
- **Conduct** – online behaviour that increases the likelihood of, or causes, harm, including online bullying, sharing personal information, making, sending or receiving explicit or intimate images, including AI-generated or manipulated images, and other harmful online behaviour; and
- **Commerce** – risks including online gambling, inappropriate advertising, phishing, scams and other forms of financial exploitation.

The School will take account of these four areas of risk in its safeguarding arrangements, online safety education, staff training, filtering and monitoring arrangements and engagement with parents.

Inappropriate Content

Pupils may encounter online content that is inappropriate or unsuitable for their age and stage of development. The school uses filtering, monitoring and device restrictions to help minimise access to harmful or inappropriate material.

Cyberbullying

Cyberbullying is bullying that takes place online or through digital devices, including messaging platforms, social media, online games or image sharing. It can include abusive messages, humiliation, discrimination or intimidation.

Like all forms of bullying, cyberbullying can have a serious impact on a child's wellbeing. Pupils are encouraged to report any form of cyberbullying to a trusted adult and not to ignore concerns.

Online Grooming

Pupils may encounter individuals online who are not who they claim to be. Grooming is the process by which someone builds a relationship with a child online in order to manipulate, exploit or abuse them. This may take place through social media, messaging platforms, online games or other digital spaces.

Pupils are encouraged to report any signs of online grooming to a trusted adult.

Sharing Nudes and Semi-Nudes

The term 'sharing nudes and semi-nudes' refers to the sending or sharing of nude or semi-nude images, videos or live streams by children and young people under the age of 18. This may take place through social media, messaging services, online games, forums or device-to-device sharing services such as AirDrop.

Pupils are reminded that creating, possessing or sharing indecent images of anyone under the age of 18 is illegal, including where images are shared between children themselves.

Online Reputation

The internet can create a permanent record of online activity, including photographs, comments, messages and content shared publicly or privately. Pupils are encouraged to consider how their online behaviour may affect their reputation, relationships and future opportunities. This is embedded throughout the Computing curriculum and wider digital literacy education.

Extremism

Extremism is the vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty, and mutual respect and tolerance of different faiths and beliefs.

Pupils are encouraged to report any concerning online content, behaviour or communication relating to extremism to a trusted adult.

Radicalisation

Radicalisation is the process through which a person may be encouraged or influenced to adopt extremist views or beliefs. This can happen online through exposure to harmful content, communities or individuals.

Pupils are encouraged to report any concerns relating to radicalisation or extremist content to a trusted adult.

15. Artificial Intelligence (AI)

Artificial intelligence (AI) tools and technologies are becoming increasingly common in education and wider society. The school recognises the opportunities AI can provide to support learning, creativity, accessibility and productivity, while also recognising the potential safeguarding, ethical and educational risks associated with its misuse.

Staff and pupils should use AI tools safely, responsibly and critically. AI-generated content may sometimes be inaccurate, biased, inappropriate or misleading and should not be accepted uncritically as fact.

The use of AI must comply with the school's safeguarding, data protection, behaviour

and academic expectations. Users must not input personal, sensitive or confidential information into AI platforms unless approved by the school.

Pupils will be taught age-appropriate AI literacy, including:

- understanding what AI is and how it works;
- recognising the strengths and limitations of AI systems;
- evaluating the reliability and accuracy of AI-generated content;
- understanding ethical issues relating to AI, including bias, misinformation and privacy;
- using AI tools responsibly to support, rather than replace, learning and independent thinking.

Staff will receive guidance and training on the safe, effective and responsible use of AI tools to support teaching, learning and professional practice.

The school recognises that generative AI may present specific safeguarding risks, including harmful or inappropriate AI-generated content, simulated interactions, misinformation and disinformation, manipulation, deepfakes and the creation or sharing of AI-generated sexual or intimate imagery. Any safeguarding concern involving AI will be managed in accordance with the school's safeguarding procedures.

The school reserves the right to restrict or prohibit the use of particular AI tools or platforms where safeguarding, privacy, educational or operational concerns exist.

16. Monitoring

The school reserves the right to monitor the use of its IT systems, devices, internet access and communication platforms, and to retain logs of network, internet and email activity in accordance with safeguarding, security and data protection requirements.

Monitoring may include the use of automated systems to identify safeguarding concerns, inappropriate content, cybersecurity risks or breaches of school policy. Access to systems, accounts or activity logs may be reviewed where necessary for safeguarding, operational, disciplinary or security purposes.

Notting Hill Preparatory School adopts a multi-layered approach to monitoring pupils' use of technology and the internet. The majority of monitoring takes place through the direct supervision of pupils by staff in classrooms and other school environments.

Where pupils are learning remotely, staff remain vigilant during online lessons and report any incidents or concerns in accordance with the school's safeguarding procedures and the Remote Learning Safeguarding Addendum.

The effectiveness of Notting Hill Prep School's filtering and monitoring arrangements will be formally reviewed at least once every academic year. A written record of the review, the checks undertaken and any actions will be kept. The review will be led by the senior leader responsible

for filtering and monitoring, with support from the DSL and IT support. The review will include checks that filtering is operating appropriately across relevant school-managed internet-connected devices and locations, and a record of these checks and any resulting actions will be maintained.

Physical monitoring

- Physical monitoring is used in classrooms, computing rooms and other low-risk environments where staff are able to intervene immediately should an issue arise.
- Where appropriate, incidents such as unsuitable internet search results may be used as educational opportunities to reinforce safe and responsible online behaviour.
- Periodic spot checks may be carried out on pupil devices to determine whether unsuitable or inappropriate websites or materials have been accessed.

Internet and Web access monitoring

- Filtering and monitoring systems provided by LGfL are used to support safeguarding and restrict access to inappropriate content. Block and monitoring lists are reviewed and updated regularly.
- classroom.cloud software is used to support classroom monitoring and identify potentially concerning online activity. Relevant logs may be reviewed by the Heads of Digital Learning, DSL and DDSLs where appropriate.

Active or Pro-active Systems

- The school may carry out retrospective searches or reviews of user activity where necessary to investigate safeguarding, security or behavioural concerns. This may include searches based on devices, users, websites visited or categories of monitored content.
- Monitoring systems may be used to identify behaviours, communications or online activity which may present a safeguarding, wellbeing or cybersecurity concern.

17. Online safety Incident Reporting

A DSL or DDSL should be informed immediately by completing the Online safety breach log (link found in the Safeguarding icon on all school desktops) and this should then be followed up with a report on CPOMS.

Any safeguarding, cybersecurity, filtering, monitoring or inappropriate content concerns relating to the use of technology must be reported immediately to the DSL, DDSL or appropriate member of staff.

Appendix 1

IT - STAFF ACCEPTABLE USE AGREEMENT

Introduction

This agreement sets out the expectations for the safe, responsible and professional use of technology, digital systems and online platforms at Notting Hill Preparatory School.

All staff are expected to read and follow the school's IT, Online Safety and Digital Use Policy, together with all safeguarding, data protection and staff conduct policies. This agreement applies to the use of school systems and devices both on and off site, including when working remotely.

The school reserves the right to monitor the use of its systems, devices and communication platforms in accordance with safeguarding, cybersecurity, operational and data protection requirements.

Failure to comply with this agreement or related school policies may result in disciplinary action, withdrawal of access to systems and devices, and/or referral to external agencies where appropriate.

When using the school's IT equipment, I have understood and will comply with the following statements:

Account Security and Cybersecurity

I will:

- use only my own username and password to access school systems and keep login details secure;
- not share passwords or attempt to access accounts, systems or data that I am not authorised to use;
- use multi-factor authentication where required by the school;
- report any suspected data breach, phishing attempt, cybersecurity concern or unauthorised access promptly;
- not install unauthorised software, applications or hardware onto school systems or devices;
- exercise caution when opening attachments, downloading files or accessing links from unknown or untrusted sources;
- complete required cybersecurity and online safety training provided by the school.

Professional Use of Technology

I will:

- use school systems, devices and communication platforms responsibly, professionally and in accordance with school policies;
- model safe and appropriate use of technology for pupils;
- use only school-approved systems and platforms for school-related communication and learning activities;
- not access, create, store or share illegal, extremist, discriminatory, offensive or inappropriate

material using school systems or devices;

- not use school systems to bully, harass or intimidate others;
- not attempt to bypass filtering, monitoring or security systems;
- use artificial intelligence tools responsibly and critically, in line with school guidance and professional expectations;
- not input confidential, personal or sensitive information into AI platforms unless authorised by the school.

Devices and Remote Working

I will:

- use school-owned devices responsibly and exercise reasonable care in their handling, transport and storage;
- ensure that devices and accounts are locked or logged out when left unattended;
- report any loss, theft, damage or security concern involving school devices or systems promptly;
- ensure that personal devices used to access school systems have appropriate security and password protection in place;
- handle school systems, devices and information securely when working remotely or off site;
- return school-owned devices and accessories when requested or at the end of employment.

Digital Communication and Social Media

I will:

- use school-provided email accounts and communication platforms for all school-related communication with pupils, parents, carers and external agencies;
- not use personal email accounts, messaging services or social media to communicate with pupils;
- ensure that all digital communication is professional and appropriate;
- maintain appropriate privacy settings and professional conduct on personal social media accounts;
- avoid any online behaviour that may damage the reputation of the school or undermine professional standards;
- understand that school email accounts and digital communications may be monitored and may be disclosed as part of safeguarding, legal or disciplinary procedures.

Images, Video and Digital Content

I will:

- use school equipment to create or store images, video or audio relating to school activities unless explicit permission has been granted otherwise;
- not use personal devices to photograph, record or store images or recordings of pupils unless authorised in accordance with school policy;
- ensure that digital content is created, stored and shared responsibly and appropriately;
- ensure that any authorised content created on a personal device is transferred securely to a school system and deleted promptly from the personal device;

- respect copyright, intellectual property and consent requirements when using or publishing digital content.

Data Protection and Confidentiality

I will:

- handle personal, confidential and sensitive information securely and in accordance with school policies and data protection legislation;
- ensure that sensitive information is only accessed by authorised individuals;
- not leave printed or digital confidential information unattended or visible to unauthorised individuals;
- store and transfer sensitive information securely using school-approved systems and processes;
- report any concern relating to safeguarding, data protection or misuse of technology promptly through the school's reporting procedures.

Declaration:

I confirm that I have read, understood and agree to comply with the school's IT, Online Safety and Digital Use Policy and this Staff Acceptable Use Agreement.

Staff name

Signed

Date

Appendix 2

Pupil Acceptable Use Agreement

Introduction

This is to help you understand the rules of using the internet and devices in school. The school provides these systems to allow you good access to digital technologies to enhance your learning, and the school in return expects you to agree to be a responsible user.

When using the school's IT equipment, I have understood and will comply with the following statements:

Safety:

- I know that my use of systems, devices and digital communications will be monitored and that my parent/carer contacted if a member of school staff is concerned about my safety.
- I will keep my password safe and secure and I will not try to use any other person's username and password.
- I will make sure I take care of any school-owned IT equipment.
- I will not use my own memory sticks.
- I will not upgrade or install any software on school computers.
- I will return any school-owned IT equipment to the correct place when I have finished using it.
- I will not eat while using school-owned IT equipment.
- I will keep water bottles away from school-owned IT equipment.

Using the Internet:

- I will not try and get to any websites that the school has blocked access to.
- I will not play games, access social networking sites or watch entertaining videos during the school day, unless associated with a class and I have permission from my teacher.
- I will not use the Internet to view, download, send or print materials, which are unlawful, unpleasant or abusive. If I see anything like this, I will tell a teacher.
- I will always respect the privacy and ownership rights of people inside and outside of the school.

Digital Content and Social Media:

- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will be respectful and polite to or about people online.
- If I see any hurtful comments about the school, staff or pupils I will tell a teacher.
- I will not give away any of my personal details or the personal details of other users in school, over the Internet.
- I will only use school-owned equipment to create pictures, video and sound. Pictures, video and sound will not be taken without asking permission first.
- I will not publish anything online, e.g. images or pictures, without asking my teacher.

Communication:

- I will only use my school email address for schoolwork when asked to by a teacher
- When sending emails or messages on Teams, I will make sure that they are polite and sensible.
- I will not screenshot, screen record or take any form of images of Teams, lessons, or Seesaw (pre-recorded or live)

Mobile Phones and Devices:

- I will only bring my mobile phone or smart watch to school with permission from my parent and will always hand it in at Reception on arrival
- I will not store any picture or videos from school on my personal device

Agreement:

Signed:

Class:

Date:

I have read the above and agree to follow these rules when I use school systems and devices. I know that if I break any of these rules, or cause damage to devices through breaking these rules, my parent/carers may be told and the school may apply sanctions that are appropriate and proportionate to the breach in accordance with NHP's Managing Behaviour and Rewards and Sanctions policies.

Sanctions might include: increased monitoring procedures, withdrawal of the right to access NHP ICT devices, the limiting of access to internet facilities; in cases where damage is caused through reckless use or breaking of rules, a sanction may include paying for repairs.

Y3 and Y4 Form Teachers read through this agreement with the children at the beginning of the school year and sign on behalf of their class.

Y5-8 Pupils should read and sign this agreement each school year

Appendix 3

GUEST USERS IT ACCEPTABLE USE STATEMENT

Visitors using school IT systems, devices, internet access or online platforms are expected to use technology safely, responsibly and professionally at all times.

Visitors will:

- follow the school's safeguarding, data protection and online safety expectations, including awareness of the Prevent duty and GDPR/Data Protection requirements;
- use school IT systems, devices and internet access only for approved professional purposes;
- not access, create, store or share unlawful, offensive, discriminatory, extremist or otherwise inappropriate material;
- not publish or share content that could identify pupils or staff, breach confidentiality or bring the school into disrepute;
- report any safeguarding, cybersecurity or data protection concern promptly to a member of staff;
- not attempt to bypass filtering, monitoring or security systems;
- not install software, applications or updates onto school devices without permission from the Digital Learning team or IT support staff.

Access to Systems and Devices

- Visitors requiring access to school systems or devices should use approved guest accounts where provided.
- Visitors must not use another person's login details or attempt to access restricted systems or areas of the network.
- Any personal device used to access school systems or data must be password protected and appropriately secured.
- Personal devices must not be used to store personal, confidential or sensitive school information unless explicitly authorised.

Internet and Wireless Access

- Guest wireless access may be provided where appropriate and is subject to the school's filtering and monitoring systems.
- Some websites, services or online platforms may be restricted in line with safeguarding and security requirements.
- Excessive bandwidth use unrelated to the purpose of the visit should be avoided.

Handling Information and Data

- Files or information should only be transferred where necessary and for an agreed professional purpose.

- Sensitive or personal information must only be accessed, transferred or stored using secure and approved methods.
- Any suspected data breach, accidental disclosure or cybersecurity concern must be reported immediately.

Name:

Date.....

Signed: