Notting Hill Preparatory School

1.21 Policy for E-Safety (EYFS & KS1-3)

Reviewer responsible:	**DSL, with guidance from Head of Computing and Deputy Head (Academic)**		
		Date of last review:	**09/20**
Reviewed by:	**HF**	**Date of next review:**	**09/21**

Introduction

Notting Hill Preparatory School is committed to providing an e-safe learning environment where internet enabled resources may be used in order to enhance the pupils' achievement. Online technology has developed swiftly in recent years, resulting in the dramatic rise of its use in school to promote and stimulate learning. This shift in internet use not only provides greater creativity but also presents us with increased risks.

This policy ensures that safety measures are in place to protect both pupils and staff against harmful risks that may be faced when using the internet, both in school or when working remotely. Our responsibility is to set high expectations and to maintain a consistent approach to safeguarding by knowing the content of the policy and the procedures adopted and developed by the school. Any breach of this policy will be taken seriously and may result in disciplinary action.

Aims

In accordance with school procedures for safeguarding children (**see Safeguarding and Child Protection Policy**), locally agreed interagency procedures and the Education Act 2002, and **Keeping Children Safe in Education (September 2020),** the aims of this policy are:

- To ensure that pupils know how to keep them themselves safe online
- To safeguard and protect the children and staff of NHP
- To ensure that all staff and other stakeholders know the factors which pose potential risks online
- To set out the key principles expected of all members of the school community at NHP with respect to the use of computing-based technologies
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils

Roles and responsibilities

eSafeguarding is the responsibility of the whole NHP community, and everyone has a responsibility to ensure that all members of the school community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute:

<u>Senior Management</u>

- The DSL is ultimately responsible for eSafeguarding provision for all members of the school community, working with the Head and members of SMT
- All safeguarding issues will be dealt with following the procedures within this policy and the Child Protection and Safeguarding procedures in the Safeguarding and Child Protection Policy. The DSL is the first point of contact in School for all safeguarding matters
- The DSL is responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their eSafeguarding roles
- The DSL should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident

- The DSL should take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures

Head of Computing

- To promote an awareness and commitment to eSafeguarding throughout the school
- To support the DSL in the day-to-day management for eSafeguarding within school and to have a supporting role in establishing and reviewing the school eSafeguarding policies and procedures
- To communicate regularly with school technical staff
- To communicate regularly with the Senior Management Team
- To feed into the DSL's safeguarding reports to the Board of Governors
- To ensure that eSafeguarding education is embedded across the curriculum in a way which educates children in responsible internet use and digital literacy in an educative, not suppressive way
- To raise the level of awareness about safety matters with parents to ensure that the aims of the eSafeguarding Policy are fulfilled at school and home, and to help arm parents with the knowledge and confidence to help keep their children safe online

Classroom Teachers and Support Staff

- To read, understand and help promote the school's eSafeguarding policies and guidance
- To read, understand and adhere to the school Staff IT Acceptable Use Policy
- To report any suspected misuse or problem to the Head or the DSL
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc
- To embed eSafeguarding messages wherever they can when using technology to support children's learning, whether that learning happens at school or home
- To understand and use incident-reporting mechanisms that exist within the school
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of eSafeguarding issues and their responsibilities related to the use of mobile phones, cameras and handheld devices
- To safeguard and manage their own online reputation by ensuring that privacy settings of any social media platform they use are checked frequently.
- To maintain a professional level of conduct in personal use of technology at all times to help maintain public confidence in the profession

Technical Staff

- To report any eSafeguarding related issues that come to their attention to the DSL
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work

- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To be responsible for the security of the school IT system
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of unforeseen data loss or critical incident

Managing Digital Content

Thought must be given whenever images, video and sound, including the use of school-generated assets and those found on the internet, are used in school or via platforms for remote learning (e.g. Seesaw or Firefly). In order to protect our pupils, we need to be careful when sharing these images, videos and sounds online, e.g. on a blog or through Firefly. In addition, pupils should be taught to think about how they share images, video and sound online in their personal lives.

Written permission from parents or carers will be obtained for the locations listed below before photographs or video of pupils are published. This is part of the home-school agreement on entry to the school. Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents or one in a single-parent household, in order for it to be deemed valid.

The locations are as follows:

• On the school website

• On the school's Intranet

• On the school's YouTube channel – parental consent most be sought for all pupils that are involved

• In the school prospectus and other printed promotional material

• In display material that may be used around the school

• When images are recorded or transmitted on a video or via webcam in an educational conference

NHP has also put the following safeguards in place:

• We will remind pupils of safe and responsible behaviour when creating, using and storing digital images, video and sound

• We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home

• Pupils and staff will only use school equipment to create digital images, video and sound at school or for school events. In exceptional circumstances and upon the completion of a risk assessment, personal equipment may be used with permission from the Senior Management Team provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in

accompanying text online; such resources will not be published online without the permission of the staff and pupils involved. Staff should complete a risk assessment form (see Appendix 2)

• If pupils are involved, relevant parental permission will also be sought before resources are published online

• Parents may take photographs at school events. However, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites

• When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership

• During any remote learning, live lessons will be taught on the video conferencing platform, 'Zoom' or via 'Teams'. Lessons links are password protected and staff and pupils are given strict safety guidelines in the Acceptable Use Agreements (**Appendices 3 and 4**) and in the Safeguarding Covid-19 Addendum, which sits alongside the Safeguarding and Child Protection Policy.

Staff training

Our staff will receive regular information and training on e-safeguarding issues in the form of INSET and staff meetings

• As part of the induction process all new staff will receive information and guidance on the e-Safeguarding Policy and the school's Acceptable Use Policies

• All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safeguarding and know what to do in the event of misuse of technology by any member of the school community

• All staff will be encouraged to incorporate e-safeguarding activities and awareness within their curriculum areas

Passwords

Passwords are an important aspect of computer security. They are the front line of authentication for the protection of user accounts and their associated access to IT equipment and resources. A poorly chosen password may result in the compromise of a pupil's work, sensitive information regarding pupils or staff being lost or stolen or the school's network being infected or attacked.

- A secure and robust username and password convention exists for all system access: email, network access, school management information system
- All pupils will have a unique logon and a generic password to access all school Computing equipment
- Pupils from Year 6 and above will have a unique, individually chosen password
- All staff will have a unique, individually-named user account and password for access to IT equipment and information systems available within school
- Staff should be prompted to change their passwords at any time that they feel their password may have been compromised
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- All staff and pupils will be made aware of the importance of protecting access to their personal username and passwords for Computing access
- All staff will read and agree to an Acceptable Use Agreement (**Appendix 3**) and all Key Stage 2 & 3 pupils will sign a Pupil Acceptable Use Agreement (**Appendix 4**) prior to being given access to IT systems. In Key Stage 1, the teacher will explain the main terms of the

agreement in an age appropriate language to the children and sign as a class agreement. The pupil agreements should be signed at the start of each academic year

- Pupils will be reminded of the importance of not writing down system passwords
- All staff and pupils will be encouraged only to disclose their personal passwords to authorised Computing support staff when necessary and never to anyone else. All personal passwords that have been disclosed should be changed as soon as possible
- Lessons will be given to children about how to select appropriate passwords and keep them safe

Filtering Internet Access

NHP allows Internet access to staff and pupils on the grounds that it is required for either work-related purposes or for educational need. However, the school does have provision and procedures in place to remove access for individual users should it become necessary.

The Internet is a valuable tool for teaching and learning. Unfortunately, not all content that is available on the Internet is suitable for schools, so provision has to be made to ensure that a suitable, fit-for-purpose Internet filtering solution is deployed without over blocking.

- NHP uses a filtered Internet service. The filtering system is provided by LGfL (London Grid for Learning)
- NHP's Internet provision will include filtering appropriate to the age and maturity of pupils
- NHP will always be proactive regarding the nature of content, which can be viewed through the school's Internet provision
- If pupil users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Head of Computing. All incidents should be documented on the safeguarding incident form (Appendix 1) and passed on to the DSL. The incident should also be logged on CPOMS
- NHP will regularly review the filtering product for its effectiveness
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked
- The Head of Computing keeps a log of any filter breaches. The DSL has regular meetings with the Tech Support in school and the Head of Computing to review any filter breaches and discuss any other esafeguarding related issues

Email Procedures Staff (see also Social Media and Acceptable Use Policies)

School email should in no way be considered private and its use should be for school-related communication with only limited exceptions.

- Staff should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system may be monitored and checked
- Staff should not use personal email accounts for professional purposes, especially to exchange any school-related information or documents
- Whole class or group email addresses will be used in school for communication outside of the school. Staff must blind copy (BCC) when sending anything to more than one set of parents
- Access, in school, to external personal email accounts may be blocked
- Excessive social email use can interfere with learning and productivity and will be restricted in line with the school e-safeguarding and Acceptable Use Policies
- NHP gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary
- School email accounts should be the only account that is used for school-related business

- Staff will only use official school-provided email accounts to communicate with pupils, parents and carers
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses

Mobile Phones

As mobile phones have increased in sophistication, with the functionality being parallel to that of school-based desktop and laptop computers, more care has to be taken with the usage of mobile smart type devices within school. In particular, the ability for most mobile phones to connect to the Internet, via the mobile phone provider, means that pupils are now able to access, download and upload content on school premises without using the school IT network and the associated safeguards it has in place. These types of devices, if usage is not managed appropriately, pose serious challenges for schools that are trying to safeguard pupil use of the Internet within school.

- Mobile phones will not be used during lessons or formal school time
- Staff owned mobile phones should not be used in any way during lessons or formal school time. They should be switched off or silent at all times, although they should be taken to break duties (see Policy for Playground Supervision)
- The use of a mobile phone is permitted, in exceptional circumstances, for key staff (such as the Head of Computing) when needing to contact technical support urgently and no other means is readily available. For example, that member of staff may need to call someone offsite for administrator clearance when setting up audio/visual equipment. The device itself will be kept out of the clear sight of any children in the room. The use of mobile phones is also permitted for personal reasons e.g. waiting to hear about the health of a loved one etc, although staff should inform SMT of the need to keep their personal device/mobile on and not on silent.
- Mobile phones and personally owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones
- No images or videos should be taken on mobile phones
- Wifi access is permitted on devices to visitors of NHP
- Students' mobile phones will be handed in at reception at the beginning of the school day and locked. They will only be released again at sign out
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office; it would then only be released to the pupil's parent or carer

Data Protection and Information Security

NHP holds lots of information and data on pupils, families and on staff. The amount of information which schools hold is increasing all the time and, while this data can be very useful in improving the service which a school provides, the school has a duty of care for how it handles and controls access to the sensitive and personal information and data which it holds.
The handling of secured data is everyone's responsibility, whether they are an employee, volunteer, technical support or third party provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even provoke legal action. **(For further details see Policy for Date Protection).**

- The NHP community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 2018 commitments, supplementary to the EU GDPR 2018
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the EU GDPR 2018

- The school has deployed appropriate technical controls to minimize the risk of data loss or breaches
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls
- All computers that are used to access sensitive information should be logged off when unattended
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information
- All access to information systems should be controlled via a suitably complex password
- All access to the school information management system will be on a need-to-know or least privilege basis
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school
- All personal and sensitive information taken offsite will be secured through appropriate technical controls

Managing IT Systems and Access

- NHP will be responsible for ensuring that access to the IT systems is as safe and secure as reasonably possible
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date

Overarching e-safety risks, definitions, preventions and solutions

Inappropriate content	It is possible that children may come across things online which are inappropriate for their age and stage of development. In school filters and restriction settings on particular devices are used to block this content.
Cyberbullying	Cyberbullying is the act of bullying others over the internet or on a mobile phone by sending abusive emails or texts directly or by posting nasty comments or humiliating images for others to see. Cyber-bullying is a way to describe common forms of bullying such as name- calling, racism, homophobia, sexism etc., which happens online. Like any form of bullying, cyberbullying can be horrible for the children involved and hard for them to talk about. Students are encouraged to report any form of cyber-bullying to an adult and not to ignore it.
Online grooming	Pupils may meet people online who aren't who they say they are. This could take place in a game online (Many games now are linked to the internet and players across the globe.) Grooming is a word used to describe people befriending children in order to take advantage of them for sexual purposes. Grooming usually takes place over a long period of time. In cases of sexual predators and radicalization, friendships with unsuspecting children are built up over a time span of 2-3 years. Students are encouraged to report any signs of online grooming to an adult.
Sexting	The term 'sexting' is used to describe the sending and receiving of sexually explicit photos, messages and video clips, by text, email or posting them on social networking sites. Young people increasingly choose to send images and messages to their friends, partners, or even strangers they meet online.

	Students are reminded that Sexting is an illegal act when carried out: • **by children under the age of 18** • **or of children under the age of 18**
Online reputation	The internet keeps a record of everything we do online – the photos we upload, the comments other people make about us and things we buy. This is our online reputation. It's important that children and adults understand how to manage their online reputation and the impacts for them of a negative online reputation. This in embedded throughout the Computing curriculum
Extremism	The vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faith and beliefs. We also regard calls for the death of members of our armed forces as extremist. Students are encouraged to report any signs of extremism to an adult.
Radicalisation	There is a chance that a child may meet people online or visit websites that could lead them over time to adopt extreme right-wing views, and become radicalised. Curiosity could lead a child to seek out these people. As in the incidence of online grooming, an adult online could befriend a child in order to encourage them to adopt beliefs or persuade them to join groups whose views and actions are considered extreme. Students are encouraged to report any signs of radicalisation to an adult

Monitoring
Notting Hill Preparatory School adopts a multi-layered approach to monitoring pupils' use of the internet. The majority of our interactions with our pupils involves the direct supervision of activities both in the classroom and in other places. When pupils are learning remotely, staff remain vigilant during online lessons and report any incidents or anything of concern, following the school's Safeguarding procedures, as set out in the **Remote Learning Safeguarding Addendum**.

Physical monitoring

(i) Physical monitoring is used in the classroom, computing suites and other low risk environments where a teacher is able to intervene immediately should an issue arise
(ii) In such cases e.g. when an inappropriate result is returned as a result of an internet search, then it may be used as a teaching opportunity
(iii) Period spot checks to monitor the content viewed are carried out on student iPads in KS3. This is to determine whether unsuitable and/or inappropriate websites have been visited

Internet and Web access monitoring

(i) LGfL block lists are used when an established need arises. Block and monitoring lists are frequently updated by the LGfL

Active or Pro-active Systems

(i) It is possible for us to perform individual user searches to determine patterns of activity retrospectively. An individual search may be carried out on any desktop, PC or client that can connect via the internet to the LGfL. To interrogate further, the Head of Computing or a designated member of the IT team, must log on to the LGfL and go to the Webscreen 2 section of the portal. Manual reports can be run based on a range of enquiry types: IP address, URs or a specific category report may be obtained. The categories used by the LGfL include: Content, Illegal, Bullying, Child Sex Exploitation, Discrimination, Drugs/Substance Abuse, Extremism, Pornography, Self-harm, Violence and Suicide. This is a useful fact finding system

(ii) Although the school is not considered to be a high risk establishment, systems are being explored to monitor or draw attention to behaviours that might give concern in the following areas: inappropriate behaviour online, communications and materials that are being accessed.

Appendix 1

E-Safety Incident Report Form

This form should be completed if you have a concern about a child. Once completed a hard copy should be handed to the DSL ASAP and a referenced copy of it put on CPOMS. If it is deemed to be a child protection matter, then procedures for this must be strictly followed. Please see the NHP Safeguarding & Child Protection Policy ('Procedure for Staff').

This form should be kept on CPOMS by the DSL at Notting Hill Prep

Details of incident:

Date happened:
Time:
Name of person reporting incident:
If not reported, how was the incident identified?
Where did the incident occur?
□ In school/service setting □ Outside school/ setting
Who was involved in the incident?
□ child/young person □ staff member □ other (please specify
Specify concern:
Conduct Contact Content
Type of incident:
□ bullying or harassment (cyber bullying
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist,
□ sexist,
□ LGBTQ hate material,
□ religious hate material
□ terrorist material
□ drug/bomb making material
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ self-harm
□ radicalisation
□ unauthorised purchase online
□ other (please specify)

Description of incident

Nature of incident

Deliberate access
Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed □ purchased without permission
Could the incident be considered as;

□ harassment □ grooming □ cyber bullying □ breach of e-safeguarding policy
□ breach of Pupil Code of Conduct
□ **Accidental access**
Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

Staff
□ incident reported to Head/senior manager
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ e-safety policy to be reviewed/amended
□ parent informed
Please detail any specific action taken (ie: removal of equipment)
□ **Child**
□ incident reported to head teacher/senior manager
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ e-safety policy to be reviewed/amended
Any other information

Outcome of incident/investigation

Appendix 2

NOTTING HILL PREPARATORY SCHOOL

95 LANCASTER ROAD, LONDON W11 1QQ
TELEPHONE 020 7221 0727 FAX 020 7221 0332
ADMIN@NOTTINGHILLPREP.COM

Risk assessment for

Using personal devices for taking video and photographs

(Form to be returned to Lead DSL when completed)

Print Name	**Description of device**
Reason for using your personal device rather than a school device	
Dates and times personal device will be in use **From:** **To:**	
Where and how will the device be stored/ kept while containing pupil images	
When will the images be saved onto filebrowser and deleted from the device? **Date:** **Time:**	

Permission given Yes/ No **by (print name of member of SMT)** **signed**		
Confirmation device has been cleared	**Yes/ No**	**Date**
Signed (SMT member)		

Appendix 3

NOTTING HILL PREPARATORY SCHOOL

95 LANCASTER ROAD, LONDON W11 1QQ
TELEPHONE 020 7221 0727 FAX 020 7221 0332
ADMIN@NOTTINGHILLPREP.COM

IT - STAFF ACCEPTABLE USE AGREEMENT

Introduction

The use of the latest technology is actively encouraged at NHP. With this comes a responsibility to protect users and the school from abuse of the system.

This document has been developed to ensure that all staff within our school are aware of their professional responsibilities when using IT equipment and systems. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when carrying out any activity, which involves using IT equipment and information systems, either within school, or at other locations, such as home.

Personally owned iPads that are connected to our system and have a profile installed on them are considered school-owned devices in regard to this Policy.

The following guidelines are general in nature as not every possible scenario can be thoroughly described or known at this point in time.

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

<u>On School Premises:</u>

- I will access the internet and other IT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security or IT systems, to the Head of Computing.
- All passwords I create will be in accordance with the school eSafeguarding Policy. I will ensure that I use a suitably complex password for access to the internet and IT systems and that I will use a unique password for each system.
- I will not share my passwords with any colleagues or pupils within school.
- I will seek consent from the Head of Computing prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the Head of Computing.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Head of Computing.
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.
- I understand that if I do not follow all statements in this AUP and in other school policies relating to the use of IT equipment I may be subject to disciplinary action in line with the school's established disciplinary procedures.

Off -site/Remote Learning

- I will ensure that all devices taken off site, (laptops, tablets, cameras, removable media or phones) will be secured in accordance with the school's Data Protection Registration and any information-handling procedures both on and off site.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- I will secure any equipment taken off site for school trips.
- I will only use school-owned or provided portable storage (USB sticks, portable hard drives etc.).
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/password protection deployed.
- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spread sheets/other documents created from information located within the school information management system).
- I will not download or install any software from the internet or from any other media, which may compromise the school network or information situated on it without prior authorisation from the Head of Computing.
- I will return any school-owned IT equipment or software to the relevant individual within school (Head of Computing) once it is no longer required.
- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

Social Media

The internet provides a range of social media tools that allow us to interact with one another.

We understand that everyone has the right to a private life and NHP respects this, provided we follow the guidelines set out in our policies.

NHP expects staff to maintain reasonable standards in their own behaviour, such that enables them to maintain an effective learning environment and also to uphold public trust and confidence in them and their profession.

Employees should avoid any conduct, which is likely to bring the school into disrepute.

I have understood and will comply with the following statements

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- Staff must not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to SMT.

Managing Digital Content

One has to be careful whenever images, video and sound are used in school. In order to protect our pupils, we need to think about how we will share images, video and sound online, e.g. on the school website or through a blog or Firefly. In addition, pupils should be taught to think about how they share images, video and sound online in their personal lives.

To protect ourselves, we need to think about how we will take, use and store these digital resources.

I have understood and will comply with the following statements

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the eSafeguarding Policy/ Home School Agreement (or any other relevant policy).
- Under no circumstances will I use any personally owned equipment for video, sound or images without prior consent from the designated member of staff. (Member of SMT).
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and immediately deleted from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Teaching and Learning (in school and remote learning)

I have understood and will comply with the following statements

- I will support and promote the school eSafeguarding Policy at all times. I will model safe and responsible behaviour in pupils when using Computing to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.
- I will help to enforce and monitor the Remote Learning Code of Conduct for pupils during any live lessons
- I will follow the recommended security settings for Zoom lessons when teaching remotely:

General

1. Log in to your Zoom account
2. Click on **"My Account"**
3. Select **"Settings"**
4. Ensure the **"Join before host"** feature is off, this will prevent students being able to entre a meeting room without you present
5. You may want to select **"Mute participants on entry"** to offer a calmer stat to live lessons

In Meeting (Basic)

1. Turn **"Chat"** and **"Private Chat"** off. This will mean that students will not be able to see each other's messages sent to the host nor have the ability to privately message each other during the lesson
2. Ensure **"Screen Sharing"** is set to host only so that students cannot display their screens during live lessons
3. Turn off **"Annotations"** and **"Whiteboard"** so that students are not able to use annotations tools on your shared screen

In Meeting (Advanced)

1. Turn **"Breakout Rooms"** on so that the option for you to use them is available during your live lessons
2. Turn on your **"Waiting Room"** so that students wait separately to be allowed in to your live lessons

- I will report any concerns about online security or behaviour to the Head of Computing and the DSL

Email

Email is an essential communication mechanism for both staff and pupils in today's digitally-connected world. The use of email can bring significant educational benefits for any school, both for its staff and pupils. However, email use for staff and pupils needs to be thought through and appropriate safety measures put in place. The unregulated use of email could potentially lead to a safeguarding incident as the more traditional, non-technical access controls can be bypassed with ease.

School email should in no way be considered private and its use should be for school-related communication.

A school email account is provided for staff to communicate with other teaching professionals, parents and carers or any school-related third party only for official school business.

I have understood and will comply with the following statements

- I will use my school email address for all correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- I understand that all communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will not synchronise any school email account with a personally-owned handheld device.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- I understand that emails sent to external organisations will be written carefully and authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the Head, my line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile Phones and Devices

In today's digital world, communications and content are available almost anywhere at any time.

As mobile phones have increased in sophistication, with the functionality being almost parallel to that of school-based desktop and laptop computers, more care has to be taken with the usage of mobile smart type devices within school.

Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regards to inappropriate capture, use or distribution of images of pupils or staff.

I have understood and will comply with the following statements

- I will ensure that my mobile phone and any other personally owned device is switched off or switched to 'silent' mode during school hours.
- I will ensure that my Bluetooth communication is 'hidden' or switched off and my mobile phone or device will not be used during teaching periods unless a member of the SMT in emergency circumstances has granted permission.
- I will not contact any parents or pupils on my personally owned device.
- I will not use any personally owned mobile device to take images, video or sound recordings.
- I will not use messaging services to contact friends or family during teaching day

Data protection and information security

Schools hold lots of information and data on pupils, families and on staff. The amount of information which schools hold is increasing all the time and, whilst this data can be very useful in improving the

service which a school provides, the school has a duty of care for how it handles and controls access to the sensitive and personal information and data which it holds.

The handling of secured data is everyone's responsibility, whether they are an employee, volunteer, technical support or third party provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even provoke legal action.

I have understood and will comply with the following statements

- I will not leave personal and sensitive printed documents on printers within public areas of the school.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- I will log off any computers that I have used to access sensitive information.
- I will be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- I will only access information systems via a suitably complex password.

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment, which is detailed within this agreement.

Staff name_____ Signed_____

Date_____

Appendix 4

NOTTING HILL PREPARATORY SCHOOL

95 LANCASTER ROAD, LONDON W11 1QQ
TELEPHONE 020 7221 0727 FAX 020 7221 0332
ADMIN@NOTTINGHILLPREP.COM

Pupil Acceptable Use Agreement

Introduction

This document has been developed to help you understand the rules of using computers in school. You should always follow the rules set out in this policy because these rules will help keep you and your classmates safe.

When learning remotely at home, you must follow the guidelines set out in the *Pupil Code of Conduct for Remote learning.*

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

- I have read and know what the computer rules in this document mean to me.
- I will make sure that my password for the school system is difficult to guess and I will not share my password with anybody else.
- If I think someone has guessed my password I will tell the Head of Computing.
- I will not deliberately waste resources, particularly printer paper and toner.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I see anything like this I will tell my teacher immediately.
- 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 Head of Computing when I have finished using it.
- I know that my use of technology can be checked and that my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not damage any school-owned equipment.
- I will not eat or drink while using school-owned IT equipment.

Using the Internet

- I will only go on the Internet using my own username and password.
- I will not try and get to any websites that the school has blocked access to.

- I will not play games, visit chat rooms, 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, obscene or abusive.
- I will always respect the work and ownership rights of people inside and outside of the school. This includes abiding by copyright laws on music, videos, software and intellectual materials.

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 not say nasty or hurtful things about any member of staff or pupil online.
- I will not give away any of my personal details (full name, age, date of birth, sex, address etc.) or the personal details of other users in school, over the Internet. This includes photographs or video images of me, other pupils or members of staff.
- I will never arrange to meet anyone I have only met online unless a trusted adult is with me.
- If I see any hurtful comments about the school, staff or pupils. I will take screenshots for evidence and give them to the Head teacher.
- I will not share any school photos or content from lessons, Firefly, Seesaw or school website on social media

Managing Digital Content

- 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.
- I will not screenshot, screen record or take any form of images whilst on any Zoom or Seesaw lessons (pre-recorded or live)

Email

- I will only use my school email address to contact people I know or those agreed by my teacher.
- I will take care in opening any attachments sent by email. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- When sending emails, I will make sure that they are polite and sensible.
- I will use proper etiquette when sending emails and always include a subject, write in complete sentences, and check my spelling.
- I will not use my school email account to forward chain emails.

Intranet

- I will always use proper etiquette when posting a comment (no text speak!)
- I will not write any comments that may annoy, harm or offend others.

Mobile Phones and Devices

- I will only bring my mobile phone or other devices to school with permission from my parent and will always hand it in at Reception on arrival.
- I will never use mobile phones and mobile devices (e.g. Nintendo DS) during the school day.
- I will only take pictures at school using File Browser so that I can save them into My Documents folder.
- I will not store any picture or videos from school on my personal device.

Agreement

I have read and discussed this agreement with my parents.

I agree to follow the rules set out in this AUP. I know that if I break any of these rules my parent/carer may be told and I may be banned from using computers in school for a period of time.

Form Teachers read through this agreement with the children at the beginning of the school year and sign on behalf of their class in KS1. In KS2 and 3, the children sign it themselves. Copies are kept by the Head of Computing.

Staff name_____ Signed_____

Date_____