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 POLICY

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

On School Premises:

- 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_____