Norfolk House School

ACCEPTABLE USE OF TECHNOLOGY BY PUPILS POLICY

This policy should be read alongside the Safeguarding, Data Protection and Anti-Bullying Policies.

Aim of the Policy

1. The aim of this policy is to ensure that technology, namely the internet and email, is used safely by all pupils and monitored vigilantly by staff members in order for it to support and facilitate pupil learning. We have a whole school approach to online safety with a clear policy on the use of hand-held devices in school. We believe that it is important for pupils to have an understanding of the potential dangers of internet usage and to know the correct procedures for ensuring safe online access.

2. Internet use is an important part of the school curriculum and is a necessary tool for pupils. It raises educational standards and helps to promote pupil achievement. Specifically, use of the internet allows for access to worldwide education resources and expert up-to-date resources for pupils. The School ensures that pupils remain safe when using the internet in a variety of ways.

Physical Safety

3. Pupils are taught about the dangers of electricity as part of the science and ICT programmes of study. They are advised how to behave appropriately when near electrical sockets and appliances and taught that they should not look directly at strong light sources such as the sun, lasers or projectors. Similarly, they are taught not to look directly into the light beam when working on the interactive whiteboards. Pupils are taught the correct posture for sitting at a computer and that sitting for too long can be unhealthy.

4. Pupils are taught the correct way to use ICT equipment as part of their programme of study and for Years 1 to 6 through the iPad Safe Use Agreement which they discuss in class. Pupils are advised that they should refrain from taking food and/ or any liquids anywhere near the computers. Pupils are not allowed to access the ICT Suite in break times and iPads are held securely in a locked unit, overseen by the Head of Teaching and Learning.

Network Safety and Monitoring

5. The school ensures as far as it reasonably can that the necessary filters and monitoring systems are in place to safeguard pupils from accessing potentially harmful and inappropriate material online. The following measures support this aim:

   a. DNS Filtering - all internet requests pass through a DNS filter service which is enabled by the router. This screens the requests and helps block sites which may include content such as adult themes, gambling and violence.

   b. Anti-Virus Software - ESSET anti-virus software is installed on all computers. It self-updates several times a day and its a regularly checked and maintained. Amongst other things, it helps to stop malware downloads to the computer and prevents inappropriate pop-ups.

   c. Google Safe Search - computers in the ICT Suite and within classrooms are all protected by Google Safe Search, which is enabled via the DNS filter filter service (see above). It assists with preventing adult content from appearing on searches. A notice is also provided on-screen to alert pupils of incorrect usage, should it occur.

   d. Firewall - the school's router, through which all computers connect to the internet, has a firewall enabled. Additionally, all computers have the Windows firewall enabled.

   e. Teaching of Pupils - pupils are taught that they can only access the internet when supervised by an adult and should not make any changes to network settings to the computers in the ICT Suite or elsewhere in school. Similarly, they are taught that they are not permitted to install other software or programmes on the computers as this may affect the correct functioning of the network. They are shown how to save and access their work securely and how to only print work when necessary to save resources for financial and environmental reasons and upon staff instruction. It is explained to the pupils that their use of the network can be monitored by the network administrators. Pupils are encouraged to report any inappropriate use immediately to a member of the teaching staff, all of whom receive regular updated E- Safety Training.

   f. Checking Procedures by IT Provider - the School's IT providers visit the school during each main holiday and half term period to check and update the computers in the IT Suite. They report their findings to the Headmistress.

g. IT Coordinator Checks - a monthly check is also carried out by the IT Coordinator to check the Google Chrome Browser history on the IT Suite computers. Any abnormalities should be reported to the Headmistress. The ICT Coordinator also logs any incidents of inappropriate access to websites and liaises with the Designated Safeguarding Lead/Headmistress and parents, as necessary. The log is kept in the School Office.

Teaching Internet Safety and Correct Procedure

6. Pupils are taught via the PSHCE and the ICT programme of study (Safety Online Module) that the internet contains many websites which are not child-friendly and can be offensive and inappropriate to them. Pupils should make no attempt to access a website that they know to contain unsuitable material. Examples of such material include those websites which:

   a. contains offensive language, images, games or other media;

   b. is pornographic or indecent in any degree;

   c. depicts scenes of explicit violence, degradation, humiliation or suffering;

   d. is abusive;

   e. encourages or supports the commission of a criminal offence;

   f. is unlawfully discriminatory;

   g. is intended or likely to harass or intimidate another person;

   h. represents terrorist or extremist material.

7. Pupils must not use school equipment (desktop, laptop or tablet) to post, copy, share, forward or display material of the type referred to above. Members of staff in charge of pupils who have access to the internet ensure that they are closely supervised at all times and every computer or device used by a pupil has the parental control facility at its maximum setting.

8. Pupils must not:

   a. access material which is inappropriate for their age;

b. access any social media websites, newsgroups or any website which allows them to interact with third parties;

c. should only access those websites which are related to their studies;

d. use the internet to access terrorist and extremist material

9. Pupils must:

a. report any filtering issues immediately to a member of staff.

10. Pupils will also be taught that people who put their work on the internet may not want others to copy it, and they are advised to check that they have permission to copy work in line with copyright laws. Older pupils are taught about copyright, how to paraphrase, extract information or make it clear when something is quoted from another source, as well as how they should not present the work of others as their own. Guidance for keeping safe online is differentiated by the age of the pupil and a copy of guidance appears at the end of this policy.

11. Pupils accessing the internet at home are subject to the controls placed upon them by their parents. However, any home use of the internet made in connection with the school or school activities by any of its pupils will be subject to this policy and any breach dealt with as if the event took place in school. We expect all members of the school community to behave as positive ambassadors of the school in all school-related activities undertaken through the internet.

12. In order to teach its values and its dangers correctly, the school is mindful that its filtering and monitoring systems do not overly restrict pupils' ability to learn about its safe use.

Email Safety

13. Some pupils will have their own email accounts at home. As these are independent of the school, they do not necessarily come with the safeguards that we set for email usage. Therefore, the school does not allow the use of personalised email accounts by pupils at school or at home for school purposes. Pupils are taught that using a personalised email account in school or for school use is not permitted.

Digital Image Safety

14. The school takes digital photographs and video recordings of its pupils for a range of legitimate purposes including educational, pastoral and administrative (see the Pupil Privacy Policy published on the school's website). Guidance for taking photographs on the school's iPads is set out clearly in the Safe Use Agreement. Photographs will only be taken if a teacher has directed it as part of the learning focus. The school seeks the consent of parents annually to take, store and use video recordings of pupils for further purposes which include promoting and publicising the school and its activities. Pupils will not be identified by full name in any publication without further consent being obtained.

Avoidance of Cyber-Bullying

15. The school takes bullying very seriously and has robust procedures for identifying and dealing with it, as detailed in our Anti-Bullying Policy available on the school website or by request in hard copy. We expect all pupils to communicate with each other with respect and courtesy at all times. Pupils are taught that cyber-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. Teaching is delivered through topics in PSHCE and ICT programmes of study on a regular basis throughout the school year and repeated as a spiral to develop awareness throughout their time at the school and build resilience for themselves and their peers.

16. As part of the above teaching programme, pupils offered guidance on how to deal with aspects of bullying, including cyber-bullying, and are encouraged to speak to any member of staff in relation to any concerns. The Head of Pastoral Care will have responsibility for following up on bullying issues and noting any trends in incidents.

Use of Mobile Phones by Pupils

17. Pupils are not allowed to have mobile phones in school. In exceptional circumstances, permission should be sought from the Headmistress and, if authorised, the pupil's mobile device will be stored in the School Reception during the school day. During residential trips the use of mobile phones by pupils will not be allowed. Pupils may not use camera phones under any circumstances.

Sexting

18. Pupils are made aware of the dangers of 'sexting' via the PSCHE and ICT programmes of learning and learn that the term relates to the writing and sharing of explicit messages and imagery with people they know or may not know. They are encouraged to use safe and good practice outside school, based upon their in-school learning. Any matters reported to the school in relation to sexting are followed up quickly and appropriately according to the school's Safeguarding Policy.

Use of Hand-hand Devices by Pupils

19. Pupils in Years 1 to 6 are allowed access to the school's set of iPads to enhance their learning and devices are stored safely in a lockable unit and booked out by teaching staff, as necessary. Safe Use Agreements (attached at the end of the policy) are discussed in detail in class with their teachers which pupils sign annually. These are also shared with parents so that all parties know the expectation of safe usage. Pupils are carefully supervised at all times when using iPads.

Inadvertently Accessing Inappropriate Material

20. In the event that inappropriate material is inadvertently accessed by a pupil, the pupil is taught to report this immediately to the member of staff supervising the session. The member of staff will then note the URL of the website in question, the time it was accessed, the name(s) of any pupil(s) who viewed the material, and which computer or device was being used. They will then follow up with the ICT Subject Coordinator who will record it in a log and refer any incident to the Head of Teaching and Learning / Headmistress. This may result in the pupil not being allowed to the access the internet until reassurances are given. The school reserves the right to monitor the websites visited on all computers owned by the school without forewarning.

Signed .....
(S Palmer, Headmistress)

Signed.....
(J Challinor, Chair of Directors)

Date: January 2020

Review Date: January 2022

iPad Acceptable Use Agreement for Pupils

The procedure and information within this document applies to all iPads or any other electronic hand-held device used in school. Teachers and other staff may also set additional requirements for classroom use.

User Responsibilities

· I will take good care of any iPad I use.

· I will never leave any iPad I use unattended.

· I will keep food and drinks away from the iPad as they could cause damage to it.

· I will always use the protective covers provided for the iPads.

· I will protect the iPad by only carrying it whilst it is in its case.

· I will always use the iPad in ways which are appropriate.

· I will not drop or place heavy objects (book, laptops etc) on top of the iPad.

· I will always return the iPad as directed by the teacher at the end of the lesson.

Safeguarding and Maintaining as a Learning Tool

· I will only photograph people with their permission.

· I will follow teachers' advice when taking photographs in line with Media Consent.

· I will only use the camera or the microphone when my teacher instructs me to.

· The whereabouts of the iPad should be known at all times.

· It is a user's responsibility to keep their iPad as safe and secure as possible.

Prohibited Uses

· I will not use the iPad for personal use or access social media at any time.

· I will not use the iPad to access inappropriate websites at any time. Further details

relating to this is explained in the Acceptable Use of Technology Policy on the website.
· I will never share any images or movies of people or send messages on or between devices.

• I will not alter any aspect of the settings on the device.

Lost, Damaged or Stolen iPads

· If the iPad is lost, stolen or damaged, I will inform the teacher immediately.

This procedure will be discussed with you in class with your teacher. Please sign below to confirm that you have read, understand and agree to abide by the terms of the policy.

Name: _____

Year : _____ Date: _____