SAINT NICHOLAS SCHOOL

ICT ACCEPTABLE USE POLICY

Note: This policy applies to all sections of the school including EYFS

Reviewed July 2019 December 2021

Review Date July 2020 December 2022

1. INTRODUCTION

This policy is an extension of the School Rules, covering specifically the use of the Saint Nicholas School network and any computer equipment connected to it.

For the purpose of this document, the term mobile device will include laptops and electronic notebooks, PC tablets, , smart phones, games consoles or any other portable web-enabled computing device that can connect to the schools' WiFi network.

2. COMPUTER FACILITIES

Overview

Every pupil is issued with a username, password and an email address at the start of their School career. This provides access to the computer network and a range of standard applications (word processing, spreadsheet, database etc.) as well as online facilities such as the Internet and electronic mail. A public wireless network enables users to connect with their own mobile devices.

School ICT facilities are provided to support pupils' study in all subjects, and priority will always be given to those using computers for academic and other School-related work.

Recreational use of the network is permitted within clearly stated limits and may vary from one area of the School to another.

Access to the computer network is a privilege and it is the responsibility of pupils to restrict themselves to usage which is ethical and appropriate. **Failure to comply with this policy will result in disciplinary action.**

Those administering the School network are responsible for ensuring the security of user data, and pupils can assume that their files and information are protected from viruses and from interference by others. They should not, however, assume that their activities are completely private. ICT support staff are authorised to monitor all user accounts to ensure the security of the network; records of usage, stored files and email messages that have been sent or received may be scrutinised at any time during routine system maintenance or if there is reason to suspect misuse of the network.

General Conduct: Use of the network and ICT Rooms

- Pupils should conduct themselves in an orderly and quiet fashion, and must always show consideration for other users.
- No food or drink may be consumed in the ICT suites.
- Any damage to computers, furniture or fitments should be reported to a member of staff without delay. The same applies to any apparent malfunction of equipment.
- Pupils using computers before school, during morning break and lunch break should leave the ICT rooms in time to arrive punctually for their next timetabled commitment.
- Only one pupil should be seated and working at a computer at any one time.

- Chairs should be placed tidily in computer rooms before leaving.
- When logging on to the network (including logging on from home), a pupil must always use his or her own user identification and password. Any attempt to impersonate another user will be treated as a serious offence, as will any attempt to interfere with data stored on the network by another user. These activities are in fact illegal under UK law.
- Never, under any circumstances, use another person's account or attempt to log on as a system administrator.
- Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user. The Saint Nicholas network or other networks connected to the Internet must not be vandalised. This includes the uploading or creating of computer viruses.
- Harassment is defined as the persistent annoyance of another user, or interference with another user's work. Harassment must never occur; this includes, but is not limited to, the sending of unwanted email (see below).
- If a pupil identifies a security problem on the Saint Nicholas system a teacher must be notified immediately. The problem must not be demonstrated to other users.
- Pupils must never divulge their passwords to other pupils or to users of computers outside the School. Any pupil who suspects that this has happened accidentally should change his/her password without delay. Any pupil who is found to have shared their password/s will be subject to disciplinary action.
- Before leaving a computer, pupils must always log off the network and check that the logging out procedure is complete.
- Pupils must not attempt to gain access to the local drive of any machine or to create local accounts (administrative or otherwise).
- It is strictly forbidden to attempt to share drives, folders or files across the network.
- Only software that has been provided on the network may be run on School computers; this includes programmes run from portable storage devices including USB sticks.
- Pupils are not permitted to import or download applications or games. In many cases it is illegal to do so.
- You are reminded that it is a breach of the School Plagiarism Policy (and of the rules of examination boards) to pass off another's work as your own. This includes copying and pasting information accessed online without proper acknowledgement.
- Pupils must be aware of, and comply with, the restrictions placed on certain kinds of usage; notably the playing of games on particular machines and at particular times of the day, where priority is given to academic work (for example in the libraries).

3. INTERNET AND EMAIL

Overview

The School's Internet access is via an educational service provider who block access to web sites known to contain offensive or inappropriate material.

The filter is continually updated, though there can be no absolute guarantee that unsuitable material is never available. Pupils are given training in safe and effective use of the Internet at various stages in their School career.

Rules

General Netiquette

Pupils must not:

- Send electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable,
- Disclose to a third party the personal details of any other pupil,
- Access any inappropriate Internet site,

- Breach another person's copyright in any material,
- Upload or download any unauthorised software or attempt to run that software. In particular, hacking, encryption and other system tools are expressly forbidden,
- Purchase goods or services via the computer network,
- Use the computer network to gain unauthorised access to any other computer network,
- Attempt to spread computer viruses,
- Engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden, as of course is any threatening or obscene matter.

Personal Safety

Pupils need to be aware that thoughtless use of email and the Internet may jeopardise their personal safety either at school or outside school. Pupils should therefore:

- Be aware that any person they "meet" or communicate with online may pretend to be someone else.
- Never arrange a meeting in person with anyone they have "met" or only communicated with online without prior parental approval.
- Not respond to messages or bulletin board items that are indecent, suggestive, belligerent, discriminatory, threatening, or which make the student feel uncomfortable or unsafe in any way. If such a message is encountered the pupil should report it to his/her form teacher and parents or via an online reporting service such as ThinkUKnow (http://www.thinkuknow.co.uk),
- Remember that anything they read online may not be accurate,
- Ignore offers that involve either financial transactions or personal meetings,
- Not disclose any personal details online, such as their home address or telephone number.

4. MOBILE DEVICES

Overview

Pupils may connect mobile devices to the School's public network. This provides filtered access to the internet.

Rules

These rules apply to all mobile devices:

- Pupils may only connect their own devices to the School's public network.
- Under no circumstances should computers, printers or other devices be detached from the network to make way for a pupil's own computer or mobile device.
- No mobile device may be plugged directly into any network switch, hub or router without permission.
- The sharing of local drives, folders or files across the network is strictly forbidden.
- No servers of any description should be attached to the network.
- Pupils should ensure that their own devices are properly protected from viruses before connecting to the School public network.
- Pupils are responsible for the material that exists on or is accessed via their mobile device. The School is empowered to scrutinise, and if necessary retain for further investigation, any device which is or has been attached to the network.
- The School cannot accept responsibility for any damage, howsoever caused, to pupils' own mobile devices or their contents (files, folders etc.).
- All rules of usage for Internet access and computer usage continue to apply.

- It is the responsibility of the owner to ensure that he or she has a licence for all software installed on his or her mobile device.
- No software should be run on a mobile device during lessons which is not appropriate to that lesson.
- The use of Virtual Private Networks (VPNs) on any web enabled device connected to the Saint Nicholas School domain is strictly forbidden. Any pupil who is found to be connecting to the Schools' network via a VPN will be subject to disciplinary action.

5. IPADS

The aim of the 1:1 iPad programme is to equip pupils with the tools and resources necessary for e-learning. At Saint Nicholas School, we believe that we can use e-learning to change fundamentally the way we teach and the way students learn, allowing students to collaborate, and find innovative solutions to problems, taking control of their own learning.

Access to the School's network, whether on a school computer or a personal device:

- is provided upon the basis that users comply with the school's ICT Acceptable Use Policy.
- is a privilege and it is the responsibility of pupils to restrict themselves to usage which is ethical and appropriate: failure to comply with this policy will result in disciplinary action.

All users' responsibilities

Users may not photograph any other person, without that person's consent.

The iPad maybe subject to routine monitoring by Saint Nicholas School. Devices must be surrendered immediately upon request by any member of staff.

Users in breach of the Acceptable Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

Saint Nicholas School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.

iPads belonging to other users are not to be tampered within any manner.

If an iPad is found unattended, it should be handed into the office immediately.

Additional pupil responsibilities

If an iPad is left at home or is not charged, the user still remains responsible for completing all schoolwork.

Malfunctions or technical issues are not acceptable excuses for failing to complete school work, unless there is no other means of completion.

Pupils must not use their iPad in school corridors, if walking to school to or from school, or outside of School buildings (unless with the teachers' permission).

In the event of any disciplinary action, the completion of all class work remains the responsibility of the pupil.

Care and maintenance

The following expectations must be adhered to:

- It is a user's responsibility to keep their iPad safe and secure.
- iPads should be clearly labelled with the pupils' name.
- iPad batteries are required to be charged and be ready to use in school.
- Users must use suitable protective covers/cases for their iPad.
- The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop nor place heavy objects (books, laptops, etc.) on top of the iPad.

- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Syncing the iPad to iTunes or iCloud will be maintained by a School administrator.
- Items deleted from the iPad cannot be recovered.
- 8GB of memory must be left free for school apps.

Lost, Damaged or Stolen iPad

If the iPad is lost, stolen, or damaged, the IT Manager/Head Master must be notified immediately.

iPads that are believed to be stolen can be tracked through iCloud.

If a pupil places their iPad in their locker it is the pupil's responsibility to ensure the locker is locked.

Prohibited uses (not exclusive)

Accessing Inappropriate Materials

All material on the iPad must adhere to the ICT Acceptable Use Policy. Users are not allow to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.

Illegal Activities

It is expressly forbidden to use School's internet/e-mail accounts for personal financial or commercial gain or for any illegal activity.

Violating Copyrights

Users are not allowed to have music and install apps on their iPad.

Cameras, images & movies

Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of cameras in toilets or changing rooms, regardless of intent, will be treated as a serious violation.

Images of other people may only be made with the permission of those in the photograph.

Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of a Teacher, or in the case of staff use, a member of the Senior Leadership Team.

Use of the camera and microphone must be in accordance with permission granted by a teacher.

Passwords & codes

Users are encouraged to set a passcode on their iPad to prevent other users from misusing it.

Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.

Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.

Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the School.

Users should be aware of and abide by the guidelines set out by the School's Onliney policy.

Saint Nicholas School reserves the right to confiscate and search an iPad to ensure compliance with this Acceptable Use Policy.

Pupil use guidelines

Pupils must

- bring their iPad to all lessons. The exception is PE or Games where iPads should be locked in the students' lockers before the start the lesson,
- ensure that their iPad is fully charged before they come to school,
- always carry their iPad in a case,

In class, pupils should:

- Keep the iPad off or close the lid until directed by a member of staff,
- Only use appropriate apps for their lessons,
- Use appropriate language for all communications,
- Follow e-safety protocols ,
- Not photograph or record staff or students, unless permission has been given by staff for a particular task,
- Not play games or use social media in any lessons
- Not access Airplay without their teacher's consent.

Pupils must not contact parents or anyone else out of school during the school day.

Sanctions

Breaches of the rules appertaining to iPad use in the classroom may dealt with in stages, depending on the nature of the breach.

Stage 1

Warnings delivered by the class teacher. If a student ignores warnings an offence may move to Stage 2.

Stage 2

Demerits will be issued by the class teacher. The School may block some features of the iPad during school time for 1 or 2 weeks as a sanction.

Stage 3

Serious breaches of the rules of iPad use or the AUP will be dealt with by the SLT. Parents will be involved in the discussions. This is likely to result in a further lock down of iPad features so students have little control. Pupils may lose the right to use an iPad in school.

Users in breach of the Acceptable Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

Student contract

Before being allowed to bring their own iPad to lessons or before being loaned a school iPad, pupils must read, agree to and sign the pupil iPad pledge.

Additional requirements when loaning a school iPad

Violating Copyrights

Users are not allowed to have music and install apps on their iPad.

Malicious Use/Vandalism

Any attempt to destroy hardware, software or data will be subject to disciplinary action.

Jailbreaking

Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.