SMITHDON HIGH SCHOOL

ACCEPTABLE USE OF ICT POLICY AND GUIDANCE

Re-adopted by Local Governing Body
March 2019

Next Review Date: March 2021

ICT NETWORK AND SIMS OVERVIEW

Usernames, Passwords and Security

All members of staff are issued with:

- Network username and password. (These are also used to access the Intranet and SIMS Learning Gateway from home).
- Automatic login to SIMS (the school management information system) which ensures that the user is automatically signed into SIMS when they log onto the network.
- A username and password for gmail, the school email system. It is expected that members of staff will log into gmail at least twice a day to check their emails. All email correspondence with colleagues and students should be restricted to gmail, as the filtering system protects the user from abuse.

Individual members of staff must ensure that other users, particularly students, do not gain access to their login either by leaving a computer logged in or by sharing a password with another user. Under NO circumstances may students be allowed to use a computer which is logged in as a member of staff. This would give the student access to confidential information in SIMS as well as in the Staff only Q: drive. If a member of staff needs to leave a room in which they are logged onto a computer they should use CTRL + ALT + DEL and lock the computer.

Availability, booking and use of ICT Suites

The following summarises how the ICT suites are timetabled:

- C32, C33, C34 - main teaching rooms of the ICT department, unused periods can be booked. C34 can be booked as a whole room or C34a (front, approx 22 PCs) and C34b (back, approx 12 PCs) can be booked separately for smaller groups.
- B58 – available for advanced timetabling or ad hoc booking.
- E25 – DT ICT suite. Available for booking when not required by DT.

Library – this facility is for Key Stage 3 timetabled Library lessons and independent research by students at lunch and break times. This facility is not for use with timetabled classes.

Booking:

Departments should have identified ICT requirements within the schemes of work. Bookings for the required numbers of sessions should be requested by the end of the summer term for the next academic year. These requests will be accommodated wherever possible. Priority will be given to:

- Controlled assignments where the exam board requires the final work to be computer generated.
- Development work requiring individual student access to specialist subject software on the network.
- Online tests.

Ad hoc bookings are made via Nicola Wilson in the office and the availability/usage is posted on the Intranet.

Whether booking in advance or using ad hoc bookings you will be required to provide information about the class, number of students and purpose.

Using ICT Suites:

- ***No bags and absolutely no food or drink.***
- ***Structured lessons – students still need the structure, expectations, lesson objectives and learning outcomes.***
- ***No headphones for music whilst working (in support of policy of no ipod/mp3 players).***
- ***Students must not be allowed to disconnect equipment.***
- ***Impero is available in all ICT suites, some of the useful features are:***

    - ***monitor student use of the PC***
    - ***restrict use of internet***
    - ***restrict internet sites available***
    - ***restrict software available***
    - ***show your desktop to the students via their desktop whilst also taking control of their PC to gain their attention as you demonstrate what is required or how to use a specific aspect of the software***
    - ***take control of individual or multiple PCs to gain student attention***

    Further guidance is available in Staff Documents.

- ***Printing – students should not be printing unless you have checked their work, use print preview to ensure no blank pages, ensure name and class is on the work (using headers and footers). Students have access to black and white printers only. Colour printing is available via reprographics. Students are required to transfer their work to the designated folder in T: drive and request printing. Further guidance for students is found in the student network handbook.***

Software Availability and installation

All software on the network is either installed on the central servers or is pushed out to PCs via the servers. It is therefore relatively straightforward for software to be made available on an additional PC or in an additional room. If you have new software that you would like to be added to the network, you should log a request via the ICT Help Centre and place the installation discs and licence documentation in the ICT System Manager's pigeonhole. Original licence documents and installation discs will be held by the ICT Support department in a secure location and a copy of the installation discs will be returned to your Head of Department.

ICT Help Centre

Staff should use the ICT Help Centre which is available via the Start menu. All technical problems, equipment faults or questions should be logged here. An email response will be received indicating the status of the case. If the case cannot be resolved quickly the response will indicate what will be required and may ask for further information.

Network User Guides

User Guides for some network software and commonly performed tasks can be found on the Intranet under Staff Documents – Whole School - Network – User Guides or the Q: drive – Whole School – Network – User Guides. This is constantly updated as new guides are written.

Q: Drive – Staff Documents

The Q: drive is also available from the Intranet via Staff Documents, to allow staff to access these shared documents from home. The first level of folders of the Q: drive is locked and cannot be added to or deleted, but staff can create new folders and files at lower levels. If you place documents in the Q: drive it is your responsibility to remove them once they are no longer needed.

Intranet and SIMS Learning Gateway

The staff Intranet can be accessed from home or any Internet enabled PC by going to the following Internet address https://slg.smithdon.norfolk.sch.uk and logging in with your normal network username and password. From the Intranet you can access the Q: drive, the School Calendar, Daily Notices and SIMS Learning Gateway. The Intranet is constantly being developed and new functionality added.

Network Restrictions for Students

Some restrictions can be applied to students who misuse computers. When applying these restrictions, they should form part of a sanction and the behaviour incident logged in SIMS. The restrictions which can be applied are as follows.

- Internet blocked at all times – this can only be requested by HoY/SLT.
- Network access restricted to certain lessons - this can only be requested by HoY/SLT.
- Network access restricted at all times - this can only be requested by HoY/SLT.

For further details please refer to the User Guide in Staff Documents – Whole School – Network – User Guides.

Smithdon High School Bring Your Own Device (BYOD) Acceptable Use Policy (AUP)

What is a Personally Owned Device?

A personally owned device will include, but not be limited to, the following:

iPad, Smartphone, Nook, Kindle or other tablet PC, laptop and netbook computer
If a student is unsure if the device is acceptable they should ask a member of the school ICT team before registering the device. The policies outlined in this document are intended to cover all available 'smart' technologies and are not limited to those specifically listed.

Expectations:

The school has set out below the expectations regarding student use of their personally owned devices. All these expectations will apply to students when they are in or around the school. Misuse of a device will result in the device being banned from the network.

The entitlement to use a personal device in school is currently available to students with prior consent from the SENCo only.

To work in line with this policy, students will:

- Only use appropriate technology at the discretion of school staff.
- Use their device for educational purposes only
- Limit their use to appropriate and purposeful educational applications and/or programs on their device.
- Only access appropriate and purposeful educational files on their device.
- Be permitted to access only the school's network through their personal devices, not private networks. Students are not allowed to use their own 3G or 4G service while at school for the transmission of data.
- Be aware that the school is not liable for loss, damage, misuse, or theft of personally owned devices brought to school under any circumstances whatsoever, even if left in locked rooms (eg changing rooms).
- Observe all school internet filters.
- Not connect their devices to the local area network via an Ethernet cable.
- Only access the network using the provided wireless network.
- Not use any device as a cyber-bullying tool or for any other offensive communication.
- Use headphones when listening to audio files such as music on their device so that the volume should be kept at a level which will not disrupt others.

While they are in the classroom, students may only listen to audio files when given express permission by their teachers.

- Follow copyright laws concerning illegal copying of music, games, movies and other protected works.
- Not be allowed to use gaming consoles or gaming devices to connect to the network.
- Be prohibited from taking pictures or digital recordings of staff or students without their prior written permission. The distribution of such media will be taken very seriously.
- Never share usernames and passwords with other students or staff.

Educational Purposes:

Students will use their electronic device for educational purposes only. This may be during a classroom activity, such as researching a topic, using a calculator for mathematical problems, creating maps, note taking, planner/calendar, document creation, or connecting to electronic resources provided by the school.

Students are responsible for their personal device and must check with teaching staff or the ICT team before engaging in particular uses of technology.

Inappropriate communication:

As a school, we recognise that in order for our students to learn and develop to the best of their ability, they need (and deserve) to feel safe. We are very clear that any form of bullying, harassment or abuse is not acceptable and will work with students and parents together to address this whenever it occurs. We are also very aware of the potential for these behaviours to take place on-line. As a school, we recognise that use of IT and personal devices is very much part of 21st century living. Our policy concerning the use of personal devices in school is really clear and aims to encourage and support the safe and responsible use of technology, with clear consequences in place for any inappropriate use.

Access to the internet is of course ‘24/7’ and we recognise the potential for inappropriate on-line behaviour involving students to take place outside school and school hours. The school will address any inappropriate on-line behaviour involving any of its students, whenever it has an impact on the sense of safety and subsequently learning and development in school of other students. Any questions or concerns should be raised with the SENCo in the first instance.

Students will refrain from using their device for inappropriate communications. These include but are not limited to the following:

> bullying, threatening, obscene, profane, vulgar language and/or images which may cause damage to an individual or the school.

Students will not use their devices for the purposes of harassment, stalking or personal attacks on other students or staff. If a student is instructed to stop sending electronic communications they must do so immediately.

Security:

The School provides content filtering for student access to the Internet. However, inappropriate material may occasionally bypass the filters and be viewed by a student. Students should report the occurrence to their teacher or the ICT team. Students will be held accountable for any deliberate attempt to bypass the LGFL filters and security. All devices must be stowed away when not in use. The School strongly recommends that machines and carry cases are personalised to reduce the risk of loss.

Consequences of Violations:

Using your own device in school is a privilege, not a right. Students who do not follow the expectations for use of personal devices will lose the privilege to utilise personal devices in school for a period of time.

- First Offence - Verbal warning by Form Tutor.
- Second Offence - Loss of BYOD privileges for a week, with contact home made by the SENCo.
- Third offence - Indefinite loss of BYOD privileges.

The school reserves the right to vary these consequences in the event of a serious breach, particularly if a safeguarding issue is identified.

User protocols:

Users must respect and protect the privacy of others by:

1. Using only assigned accounts.

2. Only viewing, using, or copying passwords, data, or networks to which they are authorised.

3. Refraining from distributing private information about others or themselves.

Users must respect and protect the integrity, availability, and security of all electronic resources by:

1. Observing all Smoothwall internet filters and posted network security practices.

2. Reporting any security risks or violations they may observe to a teacher or network administrator.

3. Not destroying or damaging data, networks, or other resources which do not belong to them, without clear permission of the owner.

4. Conserving, protecting, and sharing these resources with other users.

5. Notifying a staff member or ICT team member of computer or network malfunctions.

Users must respect and protect the intellectual property of others by:

1. Adhering to copyright laws (not making illegal copies of music, games, or movies).

2. Citing sources when using others' work (not plagiarising).

Users must respect and practice the principles of community by:

1. Communicating only in ways which are kind and respectful.

2. Reporting threatening or discomforting materials to a teacher or ICT team member.

3. Not intentionally accessing, transmitting, copying, or creating material which violates the school's Behaviour Policy (such as messages/content which are pornographic, threatening, rude, discriminatory, or meant to harass).

4. Not intentionally accessing, transmitting, copying, or creating illegal material (such as obscenity, stolen materials, or illegal copies of copyrighted works).

5. Not using the resources to further other acts which are criminal or violate the school's Behaviour Policy.

6. Avoiding spam, chain letters, or other mass unsolicited mailings.

7. Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.

Users may, if in accordance with the policy above:

1. Design and post web pages and other material from school resources.

2. Communicate electronically via tools such as email, chat, text, or videoconferencing (students require a teacher's permission).

3. Install or download software, in conformity with laws and licenses, (students must be under the supervision of a teacher) for example, NearPod or Evernote/Skitch.

4. Use the resources for any educational purpose

Social, Web Tools and Collaborative Content:

Recognising the benefits which collaboration brings to education, the school may provide students with access to websites or tools to allow communication, collaboration, sharing, and messaging among users. All school rules apply to online behaviour.

Supervision and Monitoring:

School and network administrators and their authorised employees monitor the use of information technology resources to ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement agencies. The school reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The school also reserves the right to limit the time of access.

Technical support and network connections:

Students who cannot access the wireless network or have technical issues with their device should resolve this issue by working with the user manual provided with the device outside the classroom or contact the seller directly. These are not school owned devices and the school cannot allocate resources to troubleshoot connection issues or faulty devices, beyond reasonable in-house support.

Charging:

Students are responsible for ensuring that devices are charged before they come into the school.

Printing:

We are not currently able to offer direct printing facilities.

Smithdon High School Bring Your Own Device (BYOD) Acceptable Use Policy (AUP)

STUDENT APPLICATION

I wish to apply for BYOD access rights. I confirm receipt of the school policy and agree to abide by its terms and conditions. I understand that access rights may be removed at any time by the school. I will not divulge my log-in details to anyone else and will report any possible breach to the ICT manager.

Name: ……………………………………………………………………….

Tutor Group: ……………………………………………………………………….

Signature: ……………………………………………………………………….

Date: ……………………………………………………………………….