Stanford Lake College

Policy Title	IT ACCEPTABLE USE POLICY
Author	AM Redfern
Date of First Issue	March 2020
Date of Amendments	Nov 2020
Date of Approval Letaba Educational Trust	Sep 2020

IT ACCEPTABLE USE POLICY

Stanford Lake College is dependent on its technology resources and the information that is accessed via those resources. Much of that information is provided by means of our School Data Network and the internet itself. While these networks, local and worldwide, offer invaluable opportunities for sharing information and for working more efficiently, they also offer potential windows and doors into the school's data, email accounts, and other valuable and often confidential information. We all share a responsibility to operate our systems in a way that minimises the vulnerability to our learning, teaching, and administrative work.

This Acceptable Use Policy covers the use of any computer or electronic devices while on campus and/or while connected to the school's network and facilities. This includes the computing equipment and facilities provided for educational use by Stanford Lake College as well as devices brought onto campus by students, staff, parents or visitors.

Stanford Lake College provides users with access, via our computer network, to different internet facilities such as email and browsing. Additionally, students may themselves choose to, at an appropriate time, access the internet while on campus using their own equipment and connectivity methods such as via cellular phones, tablets, laptops or other portable computing devices. All people using the internet should be aware, however, that some information accessible via the internet contains items that are illegal, defamatory and/or potentially offensive. The internet is a large, unregulated, global network where it is possible to find controversial material or sources of behaviour. This includes pornographic or sexually explicit material, as well as violence, profanity and unacceptable or offensive behaviour in private communication facilities such as emails, chat rooms and social media sites

While the intentions of the school are to make internet resources available through our facilities for constructive educational goals, users may find ways to access other materials. We believe that the benefits to the users in having access to this information resource outweigh the disadvantages. We will make every effort to block access to this type of information from our facilities; however, no system is completely fool proof and we believe that educating students about the dangers of explicit material is also beneficial. In addition, the school will not be able to monitor electronic data transfer to and from devices that are not connected through the school's network.

Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. However, at the school, we are also involved in setting standards and in monitoring adherence to our rules and to the school's standards of behaviour.

We have drawn up this document setting out the rules and conditions with which users must comply when using the computer facilities at Stanford Lake College. These rules also apply to the use of the users' own pieces of equipment with or without internet connectivity at Stanford Lake College. This means that usage of the user's own device with cellular phone-based connectivity (e.g. 3G) at the School is also governed by these rules.

1. Definitions

For the purpose of this document, the following definitions are used. The purpose of this section is to clarify these terms and not to redefine the general meaning of these terms.

1.1. **Electronic Devices**: Any electronic data storage, receiver, transmitter or similar device, including but not limited to cellular phones, personal digital assistants (PDAs), digital cameras, calculators, watches, laptops/notebooks, tablets and other portable computers, portable audio/video players including iPods and other MP3 players.

1.2. **Internet Access/Connectivity, Network Access/Connectivity**: Any connection to the internet, intranet or any other form of network (external or otherwise) by any applications/services/software on an electronic device. These include, but are not limited to, web browsing, email, peer-to-peer networks, chat services (including WhatsApp), social media sites, video streaming, voice-over-IP (VOIP), Bluetooth- or WiFi-based networks formed with electronic devices, etc.

1.3. **User**: Refers to any student, employee, service provider, parent, guardian or visitor that has permission to access the Stanford Lake College network.

1.4. **Student**: Refers to a registered pupil of Stanford Lake College.

1.5. **DoS attack**: A Denial-of-Service attack is a cyber-attack in which a server, machine or network resource is made unavailable by disrupting services. This include, but is not limited to, mail Bombing which is the act of sending massive numbers of emails to a server or an account designed to overwhelm the server or create a situation whereby the account or server is no longer usable.

1.6. **Spamming**: Sending of unsolicited communication to someone.

1.7. **Network Drive**: The storage space provided to each user that is linked to their account at Stanford Lake College. Users should not expect its content to be private as the school may need to verify that unacceptable content is not stored there. However, the school will make a reasonable attempt to make sure that users only have access to their own drive. However, users are responsible for ensuring that no one knows their password since any inappropriate content will be linked to the user of the account. These accounts can be referred to as the H Drive, Resource Drive or a drive that has the same name as a user's username.

2. Usage of Users' Own Electronic Devices (BYOD)

Stanford Lake College recognises that electronic devices are an integral part of social and educational technology and that these electronic devices are also a means of security for many children, hence Stanford Lake College will allow students/pupils to be in possession of appropriate electronic devices during school hours, or at school-related functions, subject to the provisions below:

2.1. General

- Stanford Lake College cannot be held responsible for the loss or damage to electronic devices under any circumstances;
- It is the user's responsibility to ensure that their electronic device is secure at all times;
- Students will not be allowed to be in possession of any electronic device during Assessments or Examinations, unless expressly authorised. While the school may attempt to safeguard property during such times, Stanford Lake College will not be responsible for loss or damage to the same.

General Usage

- Cellular phones and other similar communication devices should be switched off and NOT on 'silent' or 'mute' or 'flight mode' during all teaching and/or organised activities, unless otherwise instructed by the member of staff in charge;
- Students may not respond to calls, SMSs, or communication or an event of any kind on these electronic devices during teaching and/or organised activities;
- Students may not make calls, send messages, access or interact with an electronic device in any way during teaching periods or organised activities, unless specifically authorised to do so by the member of staff in charge;
- Use of any devices to access the internet or any other network (external, internal or otherwise) is subject to the rules concerning Network/Internet Usage. This also applies to cellular and Bluetooth networks.
- In devices where the capturing of pictures, videos and/or sound is possible, taking photographs, video or audio recording is not permitted on campus unless it is part of the class or organised activities and that permission has been granted by the member of staff in charge.
- A student in possession of an electronic device belonging to another person without prior and direct expressed permission will be deemed to be in possession of stolen equipment.
- Students may make use of Go-Pro's during adventures activities, with permission from the member of staff in charge and/or the Head or their nominated representatives. Take note that Stanford Lake College cannot be held responsible for the loss or damage to electronic devices under any circumstances.
- Users will be given permission to connect to the School's Network and Facilities by means of username and password. These security credentials can be obtained from the personnel at the IT department.
- Users will be given access to storage space on the server. This space can be accessed by using their security credentials. Refer to paragraph 3 for the acceptable usage of this facility.

2.2. **Use of Own Electronic Devices for Educational Purposes**

Electronic devices, as specified in paragraph 1.1, may be allowed for use in the classrooms as learning instruments and if their basic purpose is educational. Stanford Lake College strives to allow students to use any equipment that enhances their educational potential, but we must also prevent any usage that may hinder students from achieving their educational goals. These rules are to make sure students make beneficial use of electronic devices at the school for educational purposes.

2.2.1. Students must first seek permission to use any electronic devices for educational purposes in class from the member of staff in charge and/or the principal or their nominated representatives. This must be done prior to the start of the class.

2.2.2. Students may not play games, music or video files on any electronic devices (whether or not permission has been granted for the use of the device as an educational tool) during class or organised activities unless the games, music or videos are part of the teaching programme and have been required by the educator as class activity.

2.2.3. As educational tools, the notion of privacy will be treated as secondary to the achievement of the overall educational purposes. Accordingly, if a member of staff or the IT Department personnel suspects that a student is using their electronic devices for purposes other than educational ones during school times and/or on the school grounds, that member of staff/personnel will be entitled to, and indeed expected to,

intervene and inspect the contents of the device to determine whether it is being used for a purpose which is contrary to the school policies.

2.3. Connecting User's Own Equipment to the School's Network and Facilities

User's own electronic devices may not be connected to the school's network and facilities without prior permission from the Head or their designated personnel. This is regardless of the location from which this is done, be it:

- remotely via the internet or other external networks;
- close to the school's campus via its wireless network;
- or within the campus itself.

2.3.1. The school may impose conditions and restrictions on electronic devices before it may be connected to the network and/or facilities. These may include the installation of appropriate software such as antivirus and antispyware.

2.3.2. The school may disconnect any user's electronic devices from the network and/or facilities at any time.

2.3.3. Users are responsible for any actions initiated from their own electronic devices regardless of the person making use of the devices at the time. Therefore, it is recommended that users do not give others permission to make use of their devices.

3. Appropriate use of Computers, Computing Facilities and Electronic Devices

Users are expected to demonstrate appropriate behaviour when:

- using the school's computer facilities and network;
- using their own electronic devices with internet/network access (whether provided by the school or by themselves) at the school just as they are in a classroom.

Communications on the internet and other external networks are often public in nature and general school rules for behaviour and communications therefore apply. Users are personally responsible for their actions in accessing and utilising the equipment, network and/or facilities. They are also expected never to access, keep or send anything that they would not want their authority figures, or other users to see. It is expected that users will comply with the specified standards and rules set out below.

3.1. Acceptable Use

Users are expected to make appropriate use of the internet facilities and connectivity on campus primarily for direct educational purpose and constructive communication with other users, provided it is not anti-social in nature. This is expected for both access provided by the school and the user's own access while on campus.

3.2. Unacceptable Use

These are provided as guidelines, but other unacceptable behaviours not outlined here are by no means excluded. The School Code of Conduct needs to be complied with at all times and that document should also be read together with this one.

The following is a list of unacceptable use of computer, computing facilities and electronic devices:

3.2.1. Using language that is considered offensive in anything the user writes or sends – this includes impolite, anti-social, profane, abusive, racist or sexist language.

3.2.2. No user may enter chat rooms or access sites or facilities that have no relevance to the project or work on which the user is working.

3.2.3. Attempting to access pornographic or sexually explicit material is forbidden.

3.2.4. Sending chain letters, e-mails or similar forms of communication is unacceptable.

3.2.5. Mail-bombing of a server or account, spamming of another person's email account, or other inappropriate email actions are unacceptable.

3.2.6. Using or attempting to use another user's login, thereby impersonating and possibly incriminating another user is forbidden. This is regarded as fraud. This also includes cases where the previous user has forgotten to log off. Should a user find that the previous user has not logged off, they must inform the member of staff in charge immediately and ask for further instructions. Under no circumstances should the user proceed to make use of the account, access files, make changes to the computer settings or files, or take other actions to impersonate the other user.

3.2.7. Users may not give their passwords to any other person. They will be held responsible for any infringements committed using their login, along with anyone else found to be using the login.

3.2.8. Attempting to hack into or interfere with any other account, including any attempt to break into the network, or spread viruses is forbidden.

3.2.9. Copying or installing any games or any other unauthorised software onto or from any part of the network including the user's personal directory is forbidden. Pirating of software, media files or content is a criminal offense, and no shareware software is allowed unless it is approved and installed by the Network Administrator.

3.2.10. Tampering with equipment belonging to the school or others, or moving them from labs, classrooms or their proper locations is forbidden. No user may be in possession of any of the school's computer equipment without written permission.

3.2.11. Altering default settings of the school's computers or installing software without expressed permission is forbidden.

3.2.12. Vandalising any equipment belonging to the school or others is forbidden.

3.2.13. Unauthorised games may not be played on the computers at any time.

3.2.14. The use of the internet during class/homework time, without permission, is forbidden.

3.2.15. No disks, flash drives, memory cards or any movable media may be plugged into any of the school's computers, printers, scanners or other electronic devices without the permission of the member of staff.

3.2.16. Crude or unacceptable sounds, text, graphics or videos will not be tolerated.

3.2.17. Crude or socially unacceptable content may not be stored on the electronic device; Illegal and malicious content of any kind, including pirated software/content, spyware, hacking tools, may not be stored on the electronic device.

3.2.18. Users are reminded that the computers and computer facilities are public areas and that the people sharing these areas with need to be respected at all times. This includes not making a noise and disturbing other learners and keeping the areas clean and tidy.

3.2.19. The appointed personnel of the IT staff need to be contacted for all queries, recommendations and the reporting of broken or out-of-order equipment.

Users who break any of the above rules are subject to the normal disciplinary structures of the school. In addition, when using the school's internal computer network, users must understand the following:

- All users are entitled to reasonable privacy of their work under normal circumstances and therefore it is an offence to use or attempt to use another user's account/password no matter what the circumstances may be.
- Storage capacity is at a premium and users are to conserve space by deleting any unnecessary emails or other material which takes up excessive storage space.
- Users should never download or install any commercial software onto network drives. All copyright laws must be obeyed.
- Users may not use any account other than their own. They have full responsibility for their account and must not share their passwords with anyone, and therefore, any violations of any part of this policy that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account.
- The IT personnel at Stanford Lake College has the right to investigate any user's email or network drive who, in their opinion, might be transgressing either the rules or the spirit of this Acceptable Use Policy.

3.3. **Possession of Unacceptable Content** – Users will be held wholly responsible for all content stored on their electronic devices and their home drive on the school's network at all times. No excuses will be accepted for unacceptable programming or content.

3.4. **Personal Safety** – In using the network and internet, users should not reveal personal information such as home addresses or telephone numbers.

3.5. **Confidentiality of User Information** – Personally identifiable information concerning users may not be disclosed or used in any way on the internet without the prior permission form the necessary authorities. Users should never give out private or confidential information about themselves or others on the internet.

4. **User Use of Interactive Web 2.0 Tools** – Online communication is critical to the students' learning of 21st Century skills, and tools such as blogging, podcasting, and chatting offer an authentic, real-world vehicle for student expression. With the use of Google Classroom, classroom blogs, podcast projects, email, chat, or other Web interactive tools, users should follow all established internet safety guidelines including:

4.1. The use of the Google Suite, blogs, podcasts or other web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web 2.0 tools. This includes — but is not limited to — profanity, racist, sexist, or discriminatory remarks.

4.2. Users using the Google Suite, the school intranet, blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.

4.3. Users should NEVER post personal information on the web without permission from the appropriate authorities (including, but not limited to, last names and personal details such as address or phone numbers, or photographs).

4.4. Users should NEVER, under any circumstances, agree to meet someone they have met over the internet.

4.5. Users should never link to websites from their blog or blog comments without reading the entire article to make sure it is appropriate for a school setting.

Users using such tools agree to not share their username or password with anyone (note that paragraph 2.2.3 supersedes this) and treat Web posting spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog or other social media site.

5. Transgression of These Rules

Transgressions of any of these rules or other relevant codes of conduct may result in the electronic device being confiscated, deactivated or set to emergency mode only by the Head, or their nominated representative. Measures will be taken as stipulated in the school's Code of Conduct. The school may not be held liable for damages to the confiscated electronic device nor will it be responsible for providing alternative devices should it be required for educational or assessment purposes during the confiscation period.

5.1. Users may also have access to the computers, computer network and/or other facilities taken away from them. The school will not be responsible for providing alternative equipment or facilities should the equipment and facilities be required for educational or assessment purposes during the penalty period.

5.2. Users, students and their parents/guardians may be held liable for damages caused by the misuse or abuse of any electronic devices for non-academic purposes. This also applies to damage to a third party's equipment, data and other property.