Policy Document

Acceptable Use of ICT Policy

For Students

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Implementation Date: January 2012</td>
<td>Review Date and Frequency: Every two Years</td>
</tr>
<tr>
<td>Rev 1: 26 January 2014</td>
<td></td>
</tr>
</tbody>
</table>
Acceptable Use of ICT Policy - Students

In order to ensure the security of the School’s Information Communication Technology (ICT) facilities and the privacy of its users, the following security measures are required. This policy operates in conjunction with St Luke’s Anglican School rules, policies and procedures.

1. General Use of ICT Facilities

1.1. The ICT facilities are provided for educational purposes. Students may be requested display their ICT device and current pages to their supervising teacher.

1.2. Illegal, immoral, unethical, nuisance or harmful activities are strictly forbidden. Specifically, users are not to:
   1.2.1. access, publish or distribute information/data or participate in activities that are illegal, immoral, unethical or that contravene The St Luke’s Way
   1.2.2. attempt and/or participate in attempts to harm or destroy data of any Internet or School Network user
   1.2.3. knowingly access, publish and/or distribute information/data or act in a way that may harm others
   1.2.4. harass, menace or bully other users on the Internet or School Network (as supported by the Student Anti-bullying)
   1.2.5. log onto the network using another person’s user name or password
   1.2.6. breach copyright including, but not limited to, illegally copying, distributing or sharing software, images, video, music or other published works.
   1.2.7. create and/or distribute programs designed to negatively affect a user’s computer performance.

1.3. Users are not permitted to install software on School computers.

1.4. Users may not engage in activities that are detrimental to others. This includes, but is not limited to the following:
   1.4.1. downloading or printing large files
   1.4.2. impersonating other people.

1.5. Users are expected to abide by the following rules of etiquette:
   1.5.1. Be polite.
   1.5.2. Use appropriate language. Do not swear or use vulgar language.
   1.5.3. Do not reveal your personal contact details (or anyone else’s).

1.6. All information on the Internet should be considered to be copyright and should be treated accordingly.

1.7. All information accessed via the School’s Network should be considered confidential, unless explicitly marked otherwise.

   It is prohibited to publish pictures or videos of other people without their permission and/or the copyright owner’s. This includes posting images and videos of students in the School’s uniform unless permission has been granted by the Student Director, Head of School or Principal.

2. External File Access

External access is provided to allow increased access to files and information stored on the School’s Network.

2.1. Users are not to attempt any action that would contravene assessment policies and procedures.

2.2. Users are strongly advised not to transfer large files (larger than 10MB) via external access. Alternate technologies should be used, such as USB memory sticks.

3. School Computers [desktops, laptops and other forms of ICT]

3.1. Users must report any physical problems with School computers to a teacher and/or the Information Technology Department as soon as it is noticed.

3.2. Care must be taken when using or carrying a laptop. Movement of the machines is to be via the laptop trolleys only. These are housed in the School’s Resource Centre.
3.3. Interference with School computers and cabling is viewed as vandalism.
3.4. Students are to only access computers designated for student use.

4. Personal Technologies
[netbooks, laptops, ipods, MP3s, Smartphones and others forms of ICT]

Students bring personal technology to school at their own risk. The use and security of the equipment is the responsibility of the student and the School accepts no responsibility in the event of loss or damage. The use of personal technology in any way during class time or school activities is at the discretion of the supervising teacher. In order to avoid disrupting or distracting others (staff and students) personal technology must be set to silent while at school. This applies in the grounds as well as in class.

Photographs and video may not be taken (with any form of camera) of any person without their expressed permission at that time, and recordings made at the School must not be posted on any website without permission of the Student Director, Head of School or Principal.

Students who photograph or video inside the toilets or change areas may have their enrolment cancelled and may be subject to legal action.

Students are permitted, for educational purposes, to access the School's Wireless Network facilities using personal technologies such as laptops, notebooks, tablets, smart phones and other devices. In addition to this Policy, the use of personal technology is subject to the following:

4.1. Equipment must satisfy minimum hardware, operating system and software specifications (as outlined by the Information Technology Department).
4.2. IT Support staff may require access to the technology to activate network access.
4.3. Students must have anti-virus software installed (where possible). Virus definitions and software version must be kept up-to-date. Although virus protection facilities are in place on School hardware, the School is not responsible for viruses transferred to personal technology.
4.4. Activity on the School’s Network facilities is monitored continuously.
4.5. Any use of personal technology that infringes this Policy or other School rules, policies and procedures may result in disciplinary action, including suspension of the student, cancellation of access, or cancellation of enrolment.
4.6. Students may be asked to login to their device in the presence of a teacher if they are suspected of contravening this policy.

5. Email Access

Email and document sharing is provided to promote communication for educational and administrative purposes. Students must use the School's Webmail service for email.

5.1. Emails must be checked regularly. Unwanted messages should be deleted.
5.2. School email accounts will remain activated after the student has graduated so that Old Saint’s students can be contacted.
5.3. Users are not to attempt the following:
    5.3.1. Distribute illegal, immoral, unethical, offensive, harmful or nuisance messages and/or attachments.
    5.3.2. Send unsolicited email messages, including but not limited to: junk mail and chain mail.
    5.3.3. Misleadingly present personal opinions as the opinions of others.
5.4. School accounts should not be used to subscribe to mailing lists and similar forms of automatic email distribution unless it is for school-related activities. Approval must be granted by the Head of Department from the relevant subject area.
5.5. Email messages should be considered to be personal and private communication. Messages should not be forwarded on to other users without the knowledge of the original author.
6. Security Responsibilities
[Users and Owners of Personal Technologies]

All users have a responsibility to support security policies and procedures.

6.1. Users must be aware of the purpose of the service and be familiar with this policy.
6.2. Under no circumstances should attempts be made to circumvent data security measures; exploit security vulnerabilities; decrypt secure connections or data; or access prohibited web sites.
6.3. Personal information/data should not be stored on the School’s Network.
6.4. Users are expected to respect the rights and privacy of other people.
6.5. All users are provided with an alphanumeric username and a password. Users are required to ensure their password is kept secure and private. Under no circumstances should the password be shared with other people. Passwords should include a reasonable level of complexity.
6.6. Users will be held responsible for all activities that originate from their accounts or personal technologies.
6.7. All security, access or performance problems should be reported to your supervising teacher or to the Information Technology Department. Suspicious incidents or problems should be reported immediately.
6.8. Illegal, immoral, unethical, nuisance or harmful activities should be reported to the Student Director or classroom teacher.

The School reserves the right to access user data as part of investigations authorised by the Principal.