Policy Document

Acceptable Use of ICT Policy

For Staff

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Implementation Date</td>
<td>Review Date and Frequency</td>
</tr>
<tr>
<td>January 2012</td>
<td>Every two Years</td>
</tr>
<tr>
<td>Rev 1: 26 January 2014</td>
<td>Responsible for Review</td>
</tr>
<tr>
<td></td>
<td>Senior Leadership Team</td>
</tr>
</tbody>
</table>
INTRODUCTION

This document sets out the security, administration and internal rules which you should observe when communicating electronically or using the IT (Information Technology) facilities provided by St Luke’s Anglican School (‘School’).

The School Computer Network and Wireless Network will be referred to as the “School’s Network” for the purposes of this policy. You should familiarise yourself with the terms of this Policy in order to minimise potential damage to you, your colleagues, students and the School, which may arise as a result of misuse of email or Internet facilities.

This Policy applies to all employees and contractors of the School. The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School’s email and Internet facilities. You are encouraged to act with caution and take into account the underlying principles intended by this Policy. If you feel unsure of the appropriate action relating to use of email or the Internet, you should contact the Principal.

1. SCHOOL PROPERTY

The School is the owner of copyright in all electronic media created by its employees, contractors and students.

2. MONITORING

From time to time, the usage of the School computers may be monitored, including emails or the history of your Internet searches. This may include electronic communications which are sent to you or by you, both internally and externally. You should structure your electronic communications in recognition of the fact that the School may from time to time have the need to examine the contents.

The School’s Network is a business and educational tool to be used primarily for business or educational purposes. You therefore have a responsibility to use these resources in an appropriate, professional and lawful manner.

All messages on the School’s Network will be treated as education or business related messages, which may be monitored. Accordingly, you should not expect that any information or document transmitted or stored on the School’s Network will be private.

If logging onto the School’s Network, you should be aware that the School is able to monitor your use of the Internet, both during school or working hours and outside of those hours. This includes the sites and content that you visit.

3. PERSONAL USE

You are permitted to use the Internet and email facilities to send and receive personal messages, provided that such use is kept to a minimum and does not interfere with the performance of your work duties. Social media should not be used by teaching staff during class time unless it is directly related to student learning. However, you should bear in mind that any use of the Internet or email for personal purposes is still subject to the same terms and conditions as otherwise described in the Policy.
In the case of shared IT (Information Technology) facilities, you are expected to respect the needs of your colleagues and use the Internet and email in a timely and efficient manner. Excessive or inappropriate use of email or Internet facilities, for example, downloads on non-work related software, for personal reasons during working hours may lead to disciplinary action.

4. CONTENT

Email correspondence should be treated in the same way as any other correspondence, such as a letter or a fax. That is, as a permanent written record this may be read by persons other than the addressee and which could result in personal liability or the School’s liability.

It is good practice to follow the School’s Email Etiquette Guidelines when sending emails.

You and/or the School may be liable for what you say in an email message. Email is neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an email may be unexpected and extremely widespread.

You should never use the Internet or email for the following purposes:
- To abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other);
- To send or receive obscene or pornographic material;
- To injure the reputation of the School in a manner that may cause embarrassment to your employer;
- To spam or mass mail or to send or receive chain mail;
- To infringe the copyright or other intellectual property rights of another person; or
- To perform any other unlawful or inappropriate act.

Email content that may seem harmless to you may in fact be highly offensive to someone else. You should be aware, therefore, that in determining whether an email falls within any of the categories listed above, or is generally inappropriate, the School will consider the response and sensitivities of the recipient of an email rather than the intention of the sender.

If you receive inappropriate material by email, you should delete it immediately and not forward it to anyone else. It would be appropriate for you to discourage the sender from sending further materials of that nature.

Comments that are not appropriate in the workplace or school environment will also be inappropriate when sent by email. Email messages can easily be misconstrued.

Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.

You should be aware that use of the School’s Network in a manner inconsistent with the Policy or in any other inappropriate manner, including but not limited to use for the purposes referred to in the third paragraph of this section of the Policy, may give rise to disciplinary action, including termination of an employee’s employment or contractor’s engagement.

Tiered Content Filtering System: The School runs a Tiered Content Filtering System. This system blocks staff access to adult content, forums, chat rooms, gambling sites, online email functions and peer-2-peer downloading.
Addition of items on the School’s Portal (http://my.stlukes.qld.edu.au/) are made by the Information Technology Department, under direction from the Heads of School, Business Manager or the Principal.

Addition of items on the School’s website (http://www.stlukes.qld.edu.au/) are made by the Information Technology Department or the Director of Public Relations under the direction of the Principal.

5. PRIVACY

In the course of carrying out your duties on behalf of the School, you may have access to, or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers.

Email should not be used to disclose personal information of another except in accordance with the Privacy Act or with proper authorisation.

The Privacy Act requires both you and the School to take reasonable steps to protect the personal information that is held from misuse and unauthorised access. We stress therefore, that you take responsibility for the security of your personal computer and not allow it to be used by an unauthorised party, which specifically includes anyone who is not an employee of the School. You will be assigned a login code and you will also select a password to use the School’s electronic network facilities. You will be prompted to update your password every 45 days, with your current password expiring after 60 days.

You should ensure that your login details are not disclosed to anyone else. We suggest that you take steps to keep these details secure. For example, you should change your password regularly and ensure that your login code and password are not kept in writing close to your working area. You are encouraged to logout when you leave your computer unattended. This will avoid others gaining unauthorised access to your personal information, the personal information of others and confidential information within the School.

In order to comply with the School’s obligations under the Privacy Act, you are encouraged to use the blind copy option (BCC) when sending emails to multiple recipients where disclosure of those persons’ email addresses will impinge upon their privacy.

In addition to the above, you should familiarise yourself with the National Privacy Principles (‘NPPs’) and ensure that your use of email does not breach the Privacy Act or the NPPs.


6. DISTRIBUTION AND COPYRIGHT

When distributing information over the School’s computer network or to third parties outside the School, you must ensure that you and the School have the right to do so, and that you are not violating the intellectual property rights of any third party. If you are unsure of whether you have sufficient authorisation to distribute the information, we recommend that you contact the author of the work or the Principal.

In particular, copyright law may apply to the information you intend to distribute and must always be observed. The copyright material of third parties (for example, software, database files, documentation,
cartoons, articles, graphic files and downloaded information) must not be distributed through email without specific authorisation to do so.

7. ENCRYPTION AND CONFIDENTIALITY

The Internet and email are insecure means of transmitting information. Therefore, items of a highly confidential or sensitive nature should not be sent via email. All outgoing email is recommended to be archived by the user.

Email sent over the Internet may be truncated, scrambled, or sent to the wrong address. There is a possibility that outgoing email sent over the Internet may arrive scrambled or truncated, may be delayed, may not arrive at all, or may be sent to the wrong address. Where outgoing email is important or urgent, you should verify that the recipient has received the email in its entirety.

All emails that are sent from your email address contain the School’s standard disclaimer message, which is shown below.

NOTICE - The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. All information contained in this email is "commercial in confidence". Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you have received this message in error please notify the sender immediately and destroy the original message.

St Luke’s Anglican School has implemented anti-virus software, and whilst all care is taken, it is the recipient’s responsibility to ensure that any attachments are scanned for viruses prior to use. There is a risk of false attribution of email. Software is widely available by which email messages may be edited or ‘doctored’ to reflect an erroneous message or sender name. The recipient may therefore be unaware that he or she is communicating with an impostor. Accordingly, you should maintain a reasonable degree of caution regarding the identity of the sender of incoming email. You should verify the identity of the sender by other means if you have concerns.

8. VIRUSES

All external files and attachments must be virus checked using scanning software before they are accessed. The Internet is a potential host for computer viruses. The downloading of infected information from the Internet is potentially fatal to the School’s computer network.

A document attached to an incoming email may have an embedded virus. Virus checking is done automatically through the virus protector software installed on the network server and other virus protective action. If you are concerned about an email attachment or a file from a personal storage device (for example, USB drive), or believe that it has not been automatically scanned for viruses, you should contact the Information Technology Department.

9. ABSENCE

In cases where you are likely to be absent from work for more than two days, you should make arrangements for your emails to be accessible by the School or ensure that an ‘out of the office reply’ is automatically set. This automatic reply will alert those trying to contact you that you are away from work and that important queries should be directed to a nominated colleague. If you require assistance in installing this feature, please contact the Information Technology Department.
10. USE OF PERSONAL TECHNOLOGIES ON THE SCHOOL’S NETWORK

(Laptops, Notebooks, Smartphones, Tablets, or other wireless devices)
If a staff member wishes to have their personal device connected to the School’s Network, protocols are in place to enforce certain restrictions. The onus is on the staff member to seek the advice of the Information Technology Department seven days prior to the planned connection.

All personal devices will be made available to the Information Technology Department upon request, to ensure there is no Malware, Viruses Adware or Spyware.

11. POLICY UPDATES AND CONCERNS

Acceptable Use of ICT - Student Policy also needs to read in conjunction with this policy.

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

The School reserves the right to update this policy as required.