ELECTRONIC COMMUNICATIONS CODE OF ETHICS

Dear Parent & Student

Lindisfarne Anglican Grammar School would like to offer your child access to electronic communications including the Internet. The students will be able to communicate with other individuals, schools and organisations within Australia and around the world through the use of the Internet, E-Mail and other on-line services.

The students will have available to them access to thousands of databases, libraries, on-line encyclopaedias and newspapers across the world. They will be able to publish stories and poetry on to the 'net', to be read by other students across the world, and will be able to down load information they may require to complete an assignment.

We believe that such access is a vital component of preparing our students to live in the 21st century. The School will accept the role of teaching your child the rights and responsibilities of being a sensible network citizen, including a Code of Ethics that is essential to living in this new global community.

The students for their part must accept that with access comes personal responsibility. As you would realise when using the Internet, access to objectionable material or material of an adult nature is possible. This policy outlines the School's stance on access to such material. Even though the school will take every precaution to prevent such access, current technology does not allow us to prevent access completely. Students must therefore take a degree of responsibility, as outlined in the policy, as the school will take a "no tolerance" approach to accessing such material. Penalties for improper use will be enforced.

Students are also able to upload (place on the Internet) any information they wish, including information of a private nature (information about themselves they may wish to share with friends). This type of information sharing can be beneficial, however, because of the nature of the Internet, the school advises parents to be vigilant re Internet use at home.

Please read the attached policy carefully with your son/daughter before signing the agreement form. The policy is to be signed by yourself and your son/daughter. There is also a section to tick if you wish your children to have no access to electronic communications from outside the school.

This policy has been adapted along the guidelines from other Independent schools throughout Australia. For further information please contact the school.
ON-LINE CONDUCT

1. Students are responsible for the proper use of the system. The use of the Internet is a privilege, not a right and inappropriate use will result in the loss of this privilege.

2. The school system will be used only for educational purposes consistent with the school's mission and goals. Software installed by the school can trace all search paths of individual users on the system. Students found using the Internet for non-school related purposes will face disciplinary action.

3. Students may not publish any material onto the Internet without the express permission of the Teacher or Network Manager. Students may not join/register with, any areas within the Internet without permission.

4. System users shall not submit, publish or display on the schools system any knowingly inaccurate and/or objectionable material.

5. System users shall not encourage the use of tobacco, alcohol or controlled substances or otherwise promote any other activity prohibited by school policy, state or federal law or not consistent with the school's rules and code of conduct.

6. Transmission of material, information or software in violation of any school policy, local state or federal law is prohibited. Entering Internet Relay Chat areas and Hot Mail sites within the Internet is prohibited. Students must use the Group Wise E-Mail, system that is provided by the school.

7. The School reserves the right to:
   (a) monitor the computer screens at all times
   (b) examine the content of all e-mail messages sent and received
   (c) ask that e-mail content be changed if deemed unacceptable.
   (d) refuse to permit the transmission of e-mail messages that are deemed unacceptable (e.g. using offensive or objectionable text or pictures)
   (e) monitor internal e-mail, which must at all times reflect the ethos of the school.
   (f) ensure all internal e-mail must carry the correct name of the sender and is sent to intended recipients (not recipients who do not need to receive the e-mail e.g. sending an e-mail to all students).

8. Forgery or attempted forgery of e-mail (both internal and external) is unacceptable. Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.

9. System users will remove electronic mail in accordance with established retention guidelines. The Network manager may remove such messages, if not attended to by the system user.

10. Students must only download files they intend to use for educational purposes and must do so in accordance with the confines of copyright laws. Students may download material onto a personal storage devise. Information downloaded onto personal storage devices must conform to copyright rules and may be inspected by the school.

11. Students may print material via the networked printer after obtaining permission from the teacher in charge. Students are allocated print credits each term.

12. Students may save their files onto their home directory where they are secured by the student’s password. The home directories and any other areas on the system remain the property of the school, and as such may be checked by the Network Manager for inappropriate files and information.
13. Deliberate attempts to degrade or disrupt system performance with outside programs (e.g. hacking programs) or attempts to bypass software designed to protect the system and its users, will be viewed as a violation of school policy and administrative regulations and may be viewed as criminal activity under applicable law. The school reserves the right to instruct students to pay costs involved in repairing damage caused by said activities, and such conduct will result in the cancellation of system use privileges.

14. The system will automatically complete a virus check on downloaded files to avoid computer viruses. The school does not guarantee that all computer viruses will be detected. The school does not accept responsibility for the downloading of viruses or other problems to computers not owned by the school. Parents should adopt a ‘virus prevention policy’ in respect of their home and work computers.

15. System users identifying a security problem on the school's system must notify the appropriate Teacher in Charge.

16. Students are not allowed to buy/order products of any nature, over the school Internet system.

17. Students will not attempt to avoid supervision of staff by turning off monitors or utilizing the ‘Alt’ ‘Tab’ controls on the keyboard. Acts such as this will be interpreted as improper use of the system and will result in disciplinary action.

18. Vandalism or any malicious attempt to harm or destroy school equipment or materials, data of other users of the school's system or any of the agencies or other networks that are connected to the Internet is prohibited. The school reserves the right to instruct students to pay costs involved in repairing damage caused by said activities, and such conduct will result in the cancellation of system use privileges.

19. Software not belonging to the school (including DVD’s & music CD’s) may not be loaded or used on any computer. Students shall not copy or load any software (including music CD’s/files), that would constitute a breach of the copyright conditions attached to that software and the use of that software.

20. Students may not enter the operating system of any computer or attempt to bypass any systems that have been setup to protect the integrity of the system. Students may not enter the operating system of the network, or change any network settings, including print manager or Netware user tools. The use of the Novell messaging system is prohibited.

21. Students may not enter the system under a name other than their own or attempt to enter the system using another person’s password. Passwords must be kept secure at all times.

22. Any student who does not conform to the code of conduct may have their privileges to operate the computer and Internet revoked for period or time. Consistent history of violations of computer use guidelines will lead to the denial of access to the computers.

23. The School will allow access to our network via a wireless link to a privately owned Lap Top on the following conditions:

   1. The user agrees to abide by the Network Code of Ethics.
   2. Insurance will be the responsibility of the student. The school will not be liable for the loss or damage to any privately owned Lap Top on school premises.
   3. The Novell Nodal Software belongs to the school and must be removed if the student leaves the school.
4. The student agrees to allow the school to inspect any data storage devices including hard drives, USB sticks etc, if deemed necessary.
5. While all care will be taken, the school will not be responsible for problems arising due to the installation of the Novell Nodal Software.
6. The Lap Top will be used for educational purposes whilst at school.

**Printing** - Print counting software is operating on our network. Every student will be allocated a complementary amount of printing, depending upon his or her year level. This amount will be advised at the beginning of each year. Excess printing above the free limit will be charged at ten cents per page.

**Internet Downloading** - Internet Cost Accounting software is operating on our network. Each student will be allocated a per megabyte amount of download from the Internet (amounts differ depending upon year level), once the amount is used, student must pay for extra credit.

**Use of Data Storage devices (including I-Pods & USB Sticks)** – Students are encouraged to use USB sticks and other data storage devices to store their files (the use of Mobile Phones for this purpose will result in immediate confiscation). The school does reserve the right to inspect any USB stick or any other devise that is capable of storing data, if that devise is bought onto school property.

**Lost Data** – Students are advised to keep a backup of all data files. Loss of data (assignments) cannot be used as an excuse for late submission (see student handbook). The school provides a secure section on the network (student’s home directory) where students can backup files kept on a portable storage devise.

**Privacy** – The School encourages an environment where students are assured that the privacy of their communications will be respected as long as they abide by the School’s Code of Ethics. However, the Network is owned by the school and the school reserves the right to monitor all areas of the network including e-mail, internet searching, drive space supplied by the school, and privately owned data storage devises (including mobile phones, lap top computers and I-Pods) used on the network.

**Disclaimer**
The School does not warrant that the functions or services performed by or that the information or software contained on the system will meet the system users requirements or that the system will be uninterrupted or error free or that defects will be corrected. The School's system is provided on an "as is as available" basis. The school does not make any warranties, whether express or implied including without limitation, those of merchant ability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.

Please keep this section for your reference. Please sign the following page and send it back to the School.
Student Section

Please return this section to the Information Resource Centre

Student Name: ________________________ Year ________ PC Class ________

I have read the above Electronic Communication and Computer User Responsibilities Policy and agree to abide by the provisions as set out. I understand that violation of the above provisions will lead to disciplinary action and suspension of system access and related privileges and will be subject to discipline in accordance with the school’s policy and regulations. I agree to allow the school or its representatives to inspect any device capable of storing data that I carry onto school property.

Student Signature: ________________________ Date: ______________

Password
Do not allow any other person access to your password. If you believe your password has been compromised, please see your Pastoral Care teacher immediately to have it changed. You will need a password for your Novell logon and a password for your e-mail account. They can be different if you wish. They must be at least 4 (four) characters, but can be up to 6 (six), and can be a combination of letters and numbers.

If you haven’t already logged onto the system please choose a password you will remember and write it below (must be at least four characters, but no more than six characters).

I would like my logon/Email password to be: __  __  __  __  __

Parent or Guardian
I have read the School's Electronic Communications and Computer User Responsibility Policy. I realise that by using the Internet, students can be exposed to material of an unacceptable nature. The School will take the necessary precautions to minimise these possibilities, and the student within the boundaries of the policy, needs to accept the responsibilities of their actions in relation to unacceptable behaviour. In consideration for the privilege of using the school’s Communication System which gives the students access to public networks, I hereby release the school, its operators and any institutions with which they are affiliated from any claims and damaged of any nature arising from my child’s use of the system.

Please tick

☐ I give permission for my son/daughter to use the system and have access to public networks

☐ I do not give permission for my son/daughter to use the system and have access to public networks

Signature: ________________________ Date: ______________

Official Use Only

<table>
<thead>
<tr>
<th>Administration Code:</th>
<th>Entered onto Network:</th>
<th>Yes / No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration on Class List:</td>
<td>Yes / No</td>
<td>Signature:</td>
</tr>
</tbody>
</table>
POLICY ADMINISTRATION

This Policy will be reviewed periodically, or in the event of any information or incident that indicates the need for a review, or following relevant legislative or organisational change.

<table>
<thead>
<tr>
<th>Date of Policy Formulation</th>
<th>March 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Adoption</td>
<td>March 2008</td>
</tr>
<tr>
<td>Date of Last Review</td>
<td>April 2010</td>
</tr>
<tr>
<td>Date of Next Review</td>
<td>April 2015</td>
</tr>
<tr>
<td>Signature</td>
<td>Reg Schmarr</td>
</tr>
<tr>
<td>Position Held</td>
<td>Director of TAS &amp; IT</td>
</tr>
</tbody>
</table>