LINDISFARNE
ANGLICAN
GRAMMAR SCHOOL

Electronic Communications Code of Ethics

Lindisfarne Anglican Grammar School believes the teaching of cybersafe and responsible online behaviour is essential in the lives of students and is best taught in partnership between home and school.

21st century students spend increasing amounts of time online, learning and collaborating. To be safe online and to gain the greatest benefit from the opportunities provided through an online environment, students need to do the right thing by themselves and others online, particularly when no one is watching.

Safe and responsible online behaviour is covered at our School through the ICDL course and the Pastoral Care program and parents/carers are requested to reinforce this behaviour at home.

Some online activities are illegal and as such will be reported to police.

Lindisfarne Anglican Grammar School uses the internet and digital technologies as teaching and learning tools. We see the internet and digital technologies as valuable resources, but acknowledge they must be used responsibly.

Your child has been asked to agree to use the wireless network, internet and mobile technologies responsibly at school. Parents and carers should be aware that the nature of the internet is such that full protection from inappropriate content can never be guaranteed.

Please read this Code carefully with your son/daughter before signing the ICT Acceptable Use Agreement Form. The Agreement is to be signed by yourself and your son/daughter.

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. Students must:
   a) not publish any material onto the Internet without the express permission of the Teacher or Network Manager
   b) protect the privacy of others and never post or forward private information about another person
   c) only take photos and record sound or video when it is part of an approved lesson
   d) seek permission from individuals involved before taking photos, recording sound or videoing them
   e) seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space
   f) be respectful in the photos taken or video captured and never use these as a tool for bullying.

3. Systems users shall not publish or display on the School's system any knowingly inaccurate and/or objectionable material.

4. Transmission of material, information or software in violation of any School policy, local state or federal law is prohibited.

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

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

7. 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.

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

9. Students may print material via the Networked printer after obtaining permission from the class teacher at the time. Students are allocated print credits each term.

10. 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 Administrator for inappropriate files and information.

11. 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.

12. 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.

13. System users identifying a security problem on the School's system must notify the class teacher at the time or Network Administrator.

14. 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.

15. Software not belonging to the School (including DVDs and music CDs) may not be loaded or used on any School computer. Students shall not copy or load any software (including music CDs and files), that would constitute a breach of the copyright conditions attached to that software and the use of that software.

16. 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.

17. 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.

18. Any student who does not conform to the Code of Conduct may have their system privileges revoked for a period of time. Consistent history of violations of the Code will lead to the denial of access to the system.

19. The School will allow access to its Network via a wireless link to a privately owned device on the following conditions:
    a) The user agrees to abide by this Code of Ethics and returns a signed ICT Acceptable Use Agreement form indicating they agree to abide by this Code of Ethics
    b) The user submits a Wireless Personal Device Connection Request form
    c) Insurance will be the responsibility of the student. The School will not be liable for the loss or damage to any privately owned personal devices on school premises
    d) The student agrees to allow the School to inspect any data storage devices, including hard drives, USB sticks etc., if deemed necessary
    e) The personal device will be used for educational or other approved purposes whilst at school
    f) The personal devices must be charged prior to entering the classroom. No charging cords are to be connected in the classrooms.

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. Once a student has reached their limit, extra printing credit can be purchased.

Use of Personal Storage Devices (including iPods, iPads, Smart Phones and USB Sticks)

Students are encouraged to use USB sticks and other data storage devices to store their files. The School does reserve the right to inspect any USB stick or any other device that is capable of storing data, if that device is brought 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 Parent and Student Guide and the School Diary).

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. The School reserves the right to monitor all areas of the Network including email, Internet searching, drive space supplied by the School and privately owned devices (including smart phones, laptop/notebook computers, iPads and iPods).

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 merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.

Code of Conduct Administration

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

Policy Administration

These procedures 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.

INFT002 Electronic Communication Code of Ethics	
Date of Formulation	April 2010
Date of Last Review	July 2016
Date of Next Review	July 2019
Owner	Gavin Kennedy
Position Held	Director of Information Services