CYBERSAFETY AT Long Bay College

CYBERSAFETY USE AGREEMENT FOR ALL SCHOOL STAFF

This document is comprised of this cover page and three sections:

Section A: Important Cybersafety Initiatives and Rules

Section B: Some Important Staff Obligations Regarding Student Cybersafety

Section C: Staff Cybersafety Use Agreement Form.

Instructions for staff

1. Please read the entire document carefully.
2. If any clarification is required, it should be discussed with the cybersafety manager or the principal before the document is signed. Additional background information on use agreements can be found on the NetSafe website www.netsafe.org.nz/ua
3. Detach Section C, sign and return it to the office.
4. It is important to retain the remaining pages for future reference.

Important terms used in this document:

*(a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies'*

*(b) **'Cybersafety'** refers to the safe use of the Internet and ICT equipment/devices, including mobile phones*

*(c) **'School ICT'** refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below*

*(d) The term **'ICT equipment/devices'** used in this document, includes but is not limited to; computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use*

*(e) '**Objectionable**' in this agreement means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment. This is intended to be inclusive of the definition used in the Films, Videos and Publications Classification Act 1993.*

Additional information can be found on NetSafe's website www.netsafe.org.nz/ua

SECTION A
IMPORTANT LONG BAY COLLEGE CYBERSAFETY INITIATIVES AND RULES

The measures to ensure the cybersafety of Long Bay College outlined in this document are based on our core values.

The school's computer network, Internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and learning programmes at Long Bay College, and to the effective operation of the school.

Our school has rigorous cybersafety practices in place, which include cybersafety use agreements for all school staff and students.

The overall goal of the school in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the school, and legislative and professional obligations. This use agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches which undermine the safety of the school environment.

1. Cybersafety use agreements

    1.1 All staff, students and volunteers, *whether or not* they make use of the school's computer network, Internet access facilities, computers and other ICT equipment/devices in the school environment, will be issued with a use agreement.

    1.2 Staff are required to read these pages carefully, and return the signed use agreement form in Section C to the school office for filing.

    1.3 The school's computer network, Internet access facilities, computers and other school ICT equipment/devices are for educational purposes appropriate to the school environment. Staff may also use school ICT for professional development and personal use which is both reasonable and appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on *or* off the school site.

    1.4 Any staff member who has a signed use agreement with the school and allows another person who does not have a signed use agreement to use the school ICT, is responsible for that use.

2. The use of any privately-owned/leased ICT equipment/devices on the school site, or at any school-related activity must be appropriate to the school environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the school site, or to any school-related activity. This also includes the use of mobile phones.

3. When using school ICT, or privately-owned ICT on the school site or at any school-related activity, users must not:

    - Initiate access to inappropriate or illegal material
    - Save or distribute such material by copying, storing, printing or showing to other people.

4. Users must not use any electronic communication (e.g. email, text) in a way that could cause offence to others or harass or harm them, put anyone at potential risk, or in any other way be inappropriate to the school environment.

5. Staff are reminded to be aware of professional and ethical obligations when communicating via ICT with students outside school hours.

6. Users must not attempt to download, install or connect any software or hardware onto school ICT equipment, or utilise such software/hardware, unless authorised by the ICT Manager.

7. All material submitted for publication on the school website/intranet(s) should be appropriate to the school environment. Such material can be posted only by those given the authority to do so by senior management.

8. All school ICT equipment/devices should be cared for in a responsible manner. Any damage, loss or theft must be reported immediately to the ICT manager.

9. All users are expected to practise sensible use to limit wastage of computer resources or bandwidth. This includes avoiding unnecessary printing, unnecessary Internet access, uploads or downloads.

10. The users of school ICT equipment and devices must comply with the Copyright Act 1994 and any licensing agreements relating to original work. Users who infringe copyright may be personally liable under the provisions of the Copyright Act 1994.

11. Passwords must be strong, kept confidential and not shared with anyone else. A strong password is at least 8 characters in length with a mix of lower case (abd . . .) and upper case (ABC . . .) letters, symbols (#*@ . . .) and numerals (123 . . .).

12. Users should not allow any other person access to any equipment/device logged in under their own user account, unless with special permission from senior management.

13. The principles of confidentiality and privacy extend to accessing, inadvertently viewing or disclosing information about staff, or students and their families, stored on the school network or any ICT device. The Ministry of Education guidelines (www.tki.org.nz/r/governance/curriculum/copyguide_e.php) should be followed regarding issues of privacy, safety and copyright associated with student material which staff may wish to publish or post on the school website.

14. Dealing with incidents

    14.1 Staff must follow procedures relating to the school cybersafety incident book.

    14.2 Any incidents involving the unintentional or deliberate accessing of inappropriate material by staff or students must be recorded in handwriting in the cybersafety incident book with the date, time and other relevant details.

    In the event of access of such material, users should:

    1. Not show others
    2. Close or minimise the window, and
    3. Report the incident as soon as practicable to the cybersafety manager.

    14.3 If an incident involves inappropriate material or activities of a serious nature, or is suspected of being illegal, it is necessary for the incident to be reported to [*the appropriate person*] IMMEDIATELY.

15. Any electronic data or files created or modified on behalf of Long Bay College on any ICT, regardless of who owns the ICT, are the property of Long Bay College.

16. Monitoring by the school

    16.1 The school may monitor traffic and material sent and received using the school's ICT infrastructures.

    16.2 The school reserves the right to deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.

    16.3 Users must not attempt to circumvent filtering or monitoring.

17. Breaches of the agreement

    17.1 A breach of the use agreement may constitute a breach of discipline and may result in a finding of serious misconduct. A serious breach of discipline would include involvement with objectionable material, antisocial activities such as harassment or misuse of the school ICT in a manner that could be harmful to the safety of the school or call into question the user's suitability to be in a school environment.

    17.2 If there is a suspected breach of the use agreement involving privately-owned ICT on the school site or at a school-related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

    17.3 Involvement with material which is deemed 'objectionable' under the Films, Videos and Publications Classification Act 1993 is serious, and in addition to any inquiry undertaken by the school, the applicable agency involved with investigating offences under the Act may be notified at the commencement, during or after the school's investigation.

18. The school reserves the right to conduct an internal audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices, or commission an independent audit. If deemed necessary, this audit will include any stored content, and all aspects of its use, including email. An audit may include any laptops provided by or subsidised by/through the school or provided /subsidised by the Ministry of Education.

Please note that conducting an audit does not give any representative of Long Bay College the right to enter the home of school personnel, nor the right to seize or search any ICT equipment/devices belonging to that person, except to the extent permitted by law.

19. Queries or concerns

    19.1 Staff should take any queries or concerns regarding technical matters to the ICT manager.

    19.2 Queries or concerns regarding other cybersafety issues should be taken to the cybersafety manager, or to the principal.

    19.3 In the event of a serious incident which occurs when the cybersafety manager and the principal are not available, another member of senior management should be informed immediately.

SECTION B
SOME IMPORTANT STAFF REQUIREMENTS REGARDING STUDENT CYBERSAFETY

1. Staff have the professional responsibility to ensure the safety and wellbeing of children using the school's computer network, Internet access facilities, computers and other school ICT equipment/ devices on the school site or at any school-related activity.
2. If staff are aware that a student has not signed a use agreement, the student will not be permitted to use school ICT unless there are special circumstances approved by the principal.
3. If staff are aware of any students who have not signed a use agreement their names should be reported to the principal, or to the cybersafety manager.
4. Staff should guide students in effective strategies for searching and using the Internet.
5. While students are accessing the Internet in a classroom situation, the supervising staff member should be an active presence. The cybersafety manager will advise about cybersafety protocols regarding Internet access by students in other situations.
6. Staff should support students in following the student use agreement. This includes:
    a. Endeavouring to check that all students in their care understand the requirements of the student agreement
    b. Regularly reminding students of the contents of the use agreement they have signed, and encouraging them to make positive use of ICT.
7. Staff are expected to follow the instructions of the cybersafety manager regarding their role in maintaining cybersafety if students of the school are permitted email accounts. (Student email accounts may involve remote access, or access to private non-school email from within the school or on the school network).

SECTION C
LONG BAY COLLEGE STAFF CYBERSAFETY USE AGREEMENT FORM

Please complete, sign, and date this Staff Use Agreement Form which confirms your agreement to follow the obligations and responsibilities outlined in this document. The key obligations and responsibilities are:

- All ICT use must be appropriate to the school environment
- Passwords will be kept confidential
- The principles of confidentiality, privacy and copyright apply.

If you have any queries about the agreement, you are encouraged to discuss them with the cybersafety manager or the principal before you sign. Once signed, this form should be returned to the school office to be passed on to the cybersafety manager for filing with staff records.

A copy of the signed form will be supplied to you.

This year the cybersafety manager at Long Bay College is Carol Maré, Deputy Principal Operations

Additional information can be found on the NetSafe website www.netsafe.org.nz/ua

Please tick one -

❑ I believe that I have sufficient knowledge to safely supervise the use made by students in my care of the school's computer network, Internet access facilities, computers and other school ICT equipment/devices.

❑ I require additional training/professional development in order to safely supervise the use made by students in my care of the school's computer network, Internet access facilities, computers and other school ICT equipment/ devices.

Use agreement

I have read and am aware of the obligations and responsibilities outlined in this Staff Cybersafety Use Agreement document, a copy of which I have been advised to retain for reference. These obligations and responsibilities relate to the cybersafety of students, the school community and the school environment.

I also understand that breaches of this Staff Cybersafety Use Agreement will be investigated and could result in disciplinary action, and where required, referral to law enforcement.

Name: .....

Role in the school: .....

Signature: .....

Date: .....