5.04 **The use of School Electronic, Communication and Information Resources Policy**

Rationale:

To ensure the safe online learning environment, where there is appropriate and effective use of the College's Electronic, Communication and Information Resources and their associated applications as well as to promote and ensure the welfare and safety of staff and students when using these resources.

Purpose:

1. The College's Electronic, Communication and Information Resources and their associated applications are part of Liston College's educational resources. As such, they are provided for the school community for educational purposes, including assisting and enhancing the delivery of the curriculum, communication, research, the presentation of material and productivity.

2. To acknowledge that the use of the College's Electronic, Communication and Information Resources and their associated applications by staff and students, is a privilege, not a right.

3. That the Board recognises that its obligations under the National Administration Guidelines (NAG 5: for a safe physical and emotional learning environment) extends to use of the internet and related technologies.

4. To ensure that staff and students are aware of what is considered to be acceptable use of the College's Electronic, Communication and Information Resources and their associated applications and the consequences when guidelines are not followed.

Guidelines

1. All staff and students using the College's Electronic, Communication and Information Resources are required to comply with this policy.

2. Training will be made available for staff that wish to use the College's Electronic, Communication and Information Resources.

3. Electronic, Communication and Information Resources include, but are not limited to:
   - Internet and the school intranet
   - Cloud based applications
   - Email facilities
   - Server hard drives, portable storage devices, flash memory, DVDs, CDs, floppy disks, MP3
   - School databases
   - Computers (including staff laptops)
   - Cameras, including web cams, digital, optical, video
   - DVD, CD, video and audio players
   - Communications devices including, school faxes, phones (including voice mails), PDA's
   - and / or other information and communications technologies and all related applications as they come into use.

4. Guidelines for the use of computer facilities will be printed in the Staff Handbook for staff and in the School Diary for students

5. All staff and students must sign the College's Computer and Internet Acceptable Use Agreement. These documents will be retained on the appropriate staff / student personal files.

6. No computer software is to be introduced to the school's network by any electronic means without permission from the Network Manager.

7. Users must take the same care in drafting an email as they would for any other communication, to protect their own reputation and that of the school

8. Staff need to ensure the suitability of all resources used and / or references made available to students. Good practice dictates that staff must check all web sites / electronic and or media prior to students accessing them, for suitability and age restrictions. Under no circumstances should material deemed to be age restricted, be made available to students under the indicative age.

9. Users are prohibited to participate in activities that are in violation of any New Zealand law. This includes but is not limited to:
    - the copying / distribution of copyright material
    - accessing / downloading / possessing / selling objectionable material (as defined by the Films, Videos and Publications Classification Amendment Act 2015, Part 1, section 3)[1] including but not limited to: by email / over the internet / hard copy.
    - accessing material where they have no right to, unless otherwise authorised to do so[2].
    - Posting, sending or forwarding media and or emails considered "hateful" and or containing, but not limited to pornographic, defamatory, offensive, racist or obscene images and or remarks – (the Harmful Digital Communications Act 2015)

10. At no time are network users to place orders for goods or services over the Internet / email using the school's name, title or funds, with the exception of those authorised to do so.

11. Using the College access to the internet / email for commercial purposes is prohibited, unless it is part of a staff member's individuals' role. All users are responsible for any legal, financial and other obligations resulting from their use of the Internet / email.

12. Liston College is not, and cannot be held responsible for the loss of material, accidental corruption or any other action that might affect transmission or loss of data.

13. Users at all times will identify themselves and not misrepresent themselves or the school.

14. The College will take all reasonable measures to restrict access to inappropriate material whenever possible using filtering, screening and other such devices. All users must not enter (or attempt to) any site on the internet that contains inappropriate or unacceptable material[2].

15. Communications, history and storage media may be monitored / checked / examined from time to time to support operational, maintenance, auditing, security and investigative activities carried out on behalf of the college. There shall be regular and random checks of individual user's Internet Browser History files as well as data files contained on the server and / or stand-alone computers / laptops.

16. If there are issues surrounding the contents, communications history, and the like on a student's personal device, such as a phone, BYOD device, storage media, reference needs to be made to the school's policy on Search and Seizure Policy prior to action being taken

17. Users of electronic communications resources must follow the appropriate school procedures when sending and receiving communications. Such users must take all proper measures to assist the security and integrity of the network. Where a user is unsure of the providence of a communication and or an attachment, or identifies it as malicious, it should be forwarded to the network engineer as soon as practical.

18. From time to time, information and or guidelines may be provided to staff and students about appropriate use of IT resources for teaching and learning purposes.

19. Where breaches of this policy occur, consequences will be applied accordingly and reported to the Principal and or the parents, the Board of Trustees, outside authorities or others as required for appropriate action

Conclusion

The Board of Trustees makes available Electronic, Communication and Information Resources to the staff and students to assist with educational purposes in the knowledge that safeguards must be present to protect data and user access to it and to provide a safe physical and emotional learning environment.

Refer to Procedures : 5.04 The use of School Electronic Communication and Information Resources

Adopted by Board of Trustees
Review Date: _____ Chairperson:_____
Reviewed: New Policy 2004/5 28/8/07 27/04/10
Next Review: 2013 – every two years

The Use of School Electronic Communication and Information Resources Policy

[1] Section 3 states that material is "objectionable" if "it describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good".

[2] This may include material which is inappropriate in the school environment (such as 'legal pornography', dangerous (such as sites for the sale of weapons), or illegal (which could include material defined in the Films, Videos and Publications Classification Act 1993, such as child pornography; or involvement with any fraudulent activity.