



Cyber-safe, Acceptable Use Policy for I.C.T @ TLC

**INFORMATION TECHNOLOGY RESOURCES
INCLUDING THE INTERNET AND ON-LINE SERVICES**

October 2010

Table of Contents

1.	Rationale.....	4
2.	Policy.....	4
2.1	Policy Development	5
2.2	Policy Scope	5
2.3	Policy Principles	6
2.4	Relevant Legislation	8
3.	Definitions.....	8
4.	Accountabilities	9
5.	Relevant Australian Laws.....	10
5.1	Copyright Act (1968) (Commonwealth)	10
5.1.1	Conduct which will infringe copyright.....	10
5.2	Trade Marks Act (1955) (Commonwealth)	11
5.3	Trade Practices Act (1974) (Commonwealth)	11
5.4	Spam Act (2003) (Commonwealth)	11
5.5	Anti-discrimination legislation	11
5.6	Defamation	11
5.7	Censorship legislation	12
5.8	Incitement to commit an offence	12
5.9	Privacy Act (1988) (Commonwealth)	12
6.	Policy Guidelines.....	12
6.1	Acceptable Use	13
6.1.1	Internet.....	13
6.1.2	Intranet & LMS (myTLC)	13
6.1.3	Email	13
6.2	Unacceptable Use	13
6.2.1	Access to Inappropriate Material.....	14
6.2.2	Personal Safety and Personal Privacy	14
6.2.3	Illegal Activities.....	14
6.2.4	System Security	14
6.2.5	Inappropriate Language	14
6.2.6	Respect for Privacy	14
6.2.7	Respecting Resource Limits.....	14
6.2.8	System Integrity.....	15
6.2.9	Plagiarism	15
6.2.10	Copyright	15
7.	Related Documents	15

Document Control

Version	Date	Authorisation (Position)
1.0	01/01/2009	Tracey Williamson (College Reception)
2.0	9/09/2010	David Kleinschmidt (IT Manager)

Table of Authorised Officers

Position	Incumbent (Date of Leaving)
Principal	Jeanette Fuller (Current)
Business Manager	David Marquet (Current)
IT Manager	David Kleinschmidt (Current)
College Secretary	Tracey Williamson (Current)

1. Rationale

The Lakes College has a statutory obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. In addition The Lakes College Board has a responsibility to be a good employer.

These three responsibilities are increasingly being linked to the use of the Internet and Information Communication Technologies (ICT), and a number of related cyber safety issues. The Internet and ICT devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school.

The Board of The Lakes College places a high priority on providing the school with Internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

However, the Board recognises that the presence in the learning environment of these technologies (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

The Board thus acknowledges the need to have in place rigorous and effective school cyber safety and acceptable use policies and practices which are directed and guided by this document.

2. Policy

The Lakes College is committed to the protection of the essential interests of the College without inhibiting the use of the information technology environment, which is intended for the benefit of students, staff and The Lakes College generally.

The Lakes College demonstrates this commitment through the development and maintenance of rigorous and effective cyber safety and acceptable use policies and practices which aim to maximise the benefits of the Internet and ICT devices/equipment to:

1. student learning
2. teacher efficiency and effectiveness
3. parent communication
4. involvement of parents and the greater school community and
5. to the effective operation of the school, while
6. Minimising and managing any risks.

The purpose of this policy is to enable staff and students to work confidently, safely and responsibly with the present and developing information and communication technologies available within the College's information infrastructure whilst safeguarding the integrity of: computers, networks, data, and associated licensing arrangements, owned or controlled by

The Lakes College. It also provides guidance to the College community on complying with The Lakes College's policies and relevant legislation; specifies practices that mitigate against unauthorised or inappropriate use; and contains information about the organisation's responsibilities and how problems will be managed.

2.1 Policy Development

Associated issues the school will address include: the need for on-going funding for cyber safety and acceptable use policies and practices through inclusion in the annual budget, the review of the school's annual and strategic planning systems, the deployment of staff, professional development and training, implications for the design and delivery of the curriculum, the need for relevant education about cyber safety and acceptable use for the school community, disciplinary responses appropriate to breaches of cyber safety and acceptable use, the availability of appropriate pastoral support, and potential employment issues.

To develop a safe and secure school environment, the board will delegate to the Principal the responsibility to achieve this goal by developing and implementing the appropriate management procedures, practices, electronic systems, and educational programmes. These will be based on the programs available from relevant government organisations and bodies in Australia and New Zealand, including but not limited to:

1. Netsafe.org (New Zealand) incorporating Hector's World and policy recommendations and guidelines.
2. Cybersmart.gov.au (Australia)
3. Staysmartonline.gov.au (Australia) incorporating Budd:e Primary and Secondary
4. AISQ.qld.edu.au (Queensland) incorporating policy recommendations and guidelines.

A process for reporting back to the Board via the Principal from the I.C.T. department will be agreed upon and established.

2.2 Policy Scope

This policy applies to the entire Lakes College community including:

1. The Lakes College Board
2. College staff (management, permanent, casual and visiting)
3. College students and their parents.

This policy is a parent document that covers all members of the college community; child documents with more detail relating to specific sub groups will be referred to without this document and are available upon request if required.

2.3 Policy Principles

- The use of the information technology and communication systems within The Lakes College carries with it responsibilities.
- The provision of information technology and communication systems by The Lakes College is to improve and enhance learning and teaching, and conduct of the business and functions of the organisation. Using information technology, accessing information, and communicating electronically can be cost-effective, timely and efficient. It is essential that use of this valuable resource be managed to ensure that it is used in an appropriate manner.
- The process by which The Lakes College seeks to manage staff and student use of information technology and communication systems is through the development and implementation of this Policy. The Policy must be followed whenever using information and communication systems.
- This Policy governs the use of organisation information technology and communication systems and includes but is not limited to:
 - Publishing and browsing on the Internet (including Intranet and Extranet);
 - Downloading or accessing files from the Internet or other electronic sources;
 - Email;
 - Electronic bulletins/notice boards;
 - Electronic discussion/news groups;
 - Weblogs ('blogs');
 - File transfer;
 - File storage;
 - File sharing;
 - Video conferencing;
 - Streaming media;
 - Instant messaging;
 - Online discussion groups and 'chat' facilities;
 - Subscriptions to list servers, mailing lists or other like services;
 - Copying, saving or distributing files;
 - Viewing material electronically; and
 - Printing material.
- No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement/contract has been signed and returned to the school.
- Use agreements also apply to the use of privately-owned/leased ICT devices/equipment on the school site, or at/for any school-related activity,

regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.

- Use agreements / contracts will cover all board employees, all students (including adult and community), and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment, such as parents, teacher trainees, external tutors and providers, contractors, and other special visitors to the school.
- The use agreements are also an educative tool and should be used as a resource for the professional development of staff.
- Use of the Internet and the ICT devices/equipment by staff, students and other approved users is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.
- Signed use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and ICT devices/equipment.
- The school has the right to monitor access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times.
- The school has the right to audit at anytime any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.
- Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Commonwealth Privacy Act 1988.
- The safety of children is of paramount concern. Any apparent breach of cyber safety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school's cyber safety practices. In serious incidents, advice will be sought from an appropriate source, such as The Australian Communications and Media Authority (ACMA – Cybersmart Initiative) and/or a lawyer with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

2.4 Relevant Legislation

- Privacy Act (1988) (Commonwealth)
- Copyright Act (1968) (Commonwealth)
- Trade Marks Act (1955) (Commonwealth)
- Trade Practices Act (1974) (Commonwealth)
- Spam Act (2003) (Commonwealth)
- Anti-discrimination legislation
- Defamation
- Censorship legislation
- Incitement to commit an offence

3. Definitions

I.C.T. or ICT: refers to the term 'Information and Communication Technologies.

Cybersafety: refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones

School or College ICT: refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices.

ICT equipment/devices: 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, video and audio players/receivers (such as portable CD and DVD players), Gaming Consoles, and any other, similar, technologies as they come into use.

Acceptable Use: This is a widely-used term to refer to policy settings within organisations to facilitate internal and external interoperability and security of information and communications infrastructure.

Authorised User: This is a term for those users authorised by an organisation to access its systems through an authentication process. This normally involves a unique identifier and associated password.

Information and Communications Resources: Information and Communications Resources are facilities, technologies and information resources used for college information processing, transfer, storage and communications.

Security Measures: Security Measures are processes, software and hardware, used by system and network administrators to ensure the confidentiality, integrity and availability of the information technology resources and data owned by the College and its authorised users.

Spam: is the abuse of electronic messaging systems to send unsolicited, undesired bulk messages. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, and mobile phone messaging spam.

Personal Communication Devices: includes any portable device that provides for communication and data collection, transport and transfer. While not an exhaustive list, Personal Communication Devices include mobile phones, notebook computers, MP3 players, Ipods, etc.

Technologies: Refers to any hardware or software that access records or transports information in any form; including

- Mobile phones
- Email
- Internet
- Intranet
- Personal Communication devices such as iPods; MP3 Players and similar devices

4. Accountabilities

The Principal is responsible to the Board of The Lakes College for the development, implementation and administration of the policy and associated procedures relating to information and communication technology and its use within the College. The Principal is also responsible for ensuring that all staff members are adequately inducted into the requirements, obligations and responsibility.

The IT Manager is responsible for monitoring the use and application of information and communication technologies by both students and staff in accordance with prevailing privacy requirements and to report any anomalies to the Principal through the Business Manager who has functional responsibility for the information and communication technology within the College.

Staff Members are responsible for working within and abiding to the guidelines contained within this policy. All staff members have a responsibility to ensure that their use of the College information and communication technology does not jeopardise the integrity, security or service levels, or harm the reputation of The Lakes College.

Students enrolled at The Lakes College are responsible for working within and abiding by the policy and its guidelines

Parents of students enrolled at The Lakes College are responsible for ensuring their enrolled children have read or had the policies read to them and understand the guiding principles of the policy so that the parents and the students can work within and abide by the policy and its guidelines.

5. Relevant Australian Laws

Users need to be aware of conduct which may breach laws outside of the College and lead to criminal or civil proceedings and/or penalties for which they will be held personally accountable. These laws include:

5.1 Copyright Act (1968) (Commonwealth)

Text (including song lyrics), computer programs, illustrations (including maps and diagrams) photographs, music recordings, videos, films and television broadcasts are all protected by Copyright. The duration of copyright protection is generally 70 years following the death of the author. A user must not copy, send or place materials on the web without permission from the copyright owner. Infringement of another person's copyright could result in personal liability for damages.

Users should assume that all materials published on the web are in copyright, unless explicitly stated otherwise. If a user wishes to include material from another webpage in one of their own pages, they should create a hypertext link pointing to the material rather than copy it. It is suggested that the permission of other webpage owners be sought prior to creating links to their pages.

5.1.1 Conduct which will infringe copyright

Examples of conduct which will infringe copyright if undertaken without the permission of the copyright owner (eg. the relevant recording company), includes but is not limited to:

- converting a CD to an audio format, such as MP3, and using it on a PC;
- downloading a film, MP3 recordings, or software from the internet using College internet access or computers;
- uploading audio files, video files, software or commercial photographs, to a College website and making these available to the public;
- providing on a College website, links to other websites that directly offer copyright infringing material or direct users to copyright infringing material, including audio files such as MP3 recordings, video files, software or commercial photographs;

- sending copyright material, including audio files, such as MP3 recordings, video files, commercial photographs or software, to another person using College e-mail;
- storing copyright material, including audio files, such as MP3 recordings, video files, commercial photographs or software, on College computers or servers.
- Copyright infringement could apply to any file format, including, but not limited to MP3.

5.2 Trade Marks Act (1955) (Commonwealth)

A user must not copy a trademark or logo belonging to another party. Trade mark infringement will expose the user to liability for damages.

5.3 Trade Practices Act (1974) (Commonwealth)

The Trade Practices Act contains provisions which prohibit passing off and misleading and deceptive conduct. If a user were to copy material from an external site onto a College website (including features such as logos and trademarks) so that persons accessing the website would believe that The Lakes College had been authorised to carry the material, this would constitute passing off or deceptive or misleading conduct.

5.4 Spam Act (2003) (Commonwealth)

Under the Act, users must not send unsolicited commercial electronic messages. Any commercial messages that are sent electronically (including email, instant messaging or telephone accounts) must include information about the individual or organisation who authorised the sending of the message and a functional unsubscribe facility.

5.5 Anti-discrimination legislation

Commonwealth and State laws and the Colleges Equal Opportunity policy prohibit sexual harassment and discrimination, vilification or victimisation on certain grounds such as race, gender, sexual preference, disability, or status as a parent or carer. College IT facilities must not be used to humiliate, intimidate or offend others on the basis of their race, gender, or any other attribute prescribed under anti-discrimination legislation.

5.6 Defamation

A user should not publish a statement about another person which could harm that other person's reputation. There is no need for the person to have been named specifically if he/she can reasonably be identified. Photographs and cartoons can also be defamatory if they hold someone up to ridicule or contempt. In a defamation case, truth is not always a defence.

5.7 Censorship legislation

Commonwealth and state laws prohibit publication of hard core pornography (in particular where it involves children, bestiality, violence, cruelty and/or exploitation). A breach of these laws would constitute a criminal offence.

5.8 Incitement to commit an offence

Users must not publish material which is an incitement to commit or instruction in crime eg, material on how to prepare explosive devices, or how to steal or provide a link to a site that offers file-sharing software, use of which is likely to result in infringement of copyright.

5.9 Privacy Act (1988) (Commonwealth)

Users must be aware that the collection of personal information including but not limited to:

- Names
- Email Addresses
- Age, Date of Birth
- Addresses

As found in common contacts lists (friend's lists) if stored on the college network may be exposed to the rules governing the collection and use of personal information as it relates to the privacy act of the commonwealth of Australia 1988.

In short the following guidelines should be acknowledged and understood if a user intends to collect and store such information:

- Obtain the information lawfully, fairly and with full consent, awareness and understanding of the individual concerned. It is important the individual understands why you want the information and how it will be used.
- Store the information securely and responsibly, and do your best to keep it up to date and relevant, removing information as soon as it is no longer needed.
- Do not disclose or share the information with other individuals or organisations without the consent of the individual concerned.

6. Policy Guidelines

The following guidelines are to be followed by all members of The Lakes College Community. They serve as the general guidelines to be adhered to by any user type in any circumstance. There may be more specific guidelines for individual circumstances which will be outlined in small additional guideline documents and notated in the Related Documents section at the conclusion of this document. It is important to note that both the following

guidelines and any specific guidelines should be read and understood by the individual before signing the acceptable use contract applicable.

6.1 Acceptable Use

The following activities are examples of responsible and acceptable use of the information and communication technologies and personal devices within The Lakes College:

6.1.1 Internet

- Engaging in or facilitating curriculum/co-curriculum based teaching and learning activities (including research and skills based learning)
 - Carrying out tasks which are specific to a person's role in The Lakes College
 - Carrying out any activity related to accomplishing official requirements, professional duties and where acceptable, professional development
-

6.1.2 Intranet & LMS (myTLC)

- Posting The Lakes College based information for general access by students and parents (including handbooks, policies, calendar of events)
 - Posting information which is specific to a class, year level or school (including subject details, assessment details, sports results etc)
 - Posting information which is specific to staff members (policies and procedures, reporting schedules, meeting schedules etc)
 - Posting daily news (including staff notices and student notices)
-

6.1.3 Email

- Communicating with individuals and groups on The Lakes College related activities'
 - Forwarding "attached" material that is The Lakes College related
 - Carbon-copying appropriately and only as required
 - Respecting the privacy of email received
 - Respecting the time that other people have to read their email
 - Advising the sender if an email has been received by mistake
-

6.2 Unacceptable Use

Any behaviour that involves the use or application of information and communication technology that is inconsistent with the values of The Lakes College as outlined in the Strategic Plan is considered unacceptable. The following uses of The Lakes College Information and communication technology and facilities are considered unacceptable. It should be noted that this is not an exhaustive list, but for the purposes of this policy, can be identified under a number of headings.

6.2.1 Access to Inappropriate Material

- Seeking to access material that is inconsistent with the ethos of The Lakes Colleges. In particular, accessing information sources that contain:
 - pornographic material
 - racist material
 - violent or harmful material including information on weaponry etc

6.2.2 Personal Safety and Personal Privacy

- Users of the network should not post personal contact information about themselves
- Meetings with persons unknown may not be arranged via the internet

6.2.3 Illegal Activities

- Gaining unauthorised access to another's files or another computer network
- Attempting to disrupt the network or to spread a computer virus intentionally
- Using the computer network to engage in an illegal act
- Threatening the safety of another person

6.2.4 System Security

- Providing a password to another person
- Downloading software without the express permission of an authorised person

6.2.5 Inappropriate Language

- Posting inappropriate language (obscene, profane, vulgar, inflammatory, threatening, disrespectful) on a web site or including it in an email
- Accessing or making prejudicial or discriminatory attacks
- Causing distress to another person eg spreading gossip

6.2.6 Respect for Privacy

- Messages are not to be forwarded on without the sender's permission
- Contact Details and other personal or private information should only be collected, stored and/or distributed with the consent of the owner.

6.2.7 Respecting Resource Limits

- Downloading large files

- Engaging in spamming (setting in place any operation which results in multiple email messages clogging a system)
- Posting chain letters
- Storing large quantities of similar files

6.2.8 System Integrity

- Attempting to disrupt services

6.2.9 Plagiarism

- Taking the ideas of others and presenting them as one's own

6.2.10 Copyright

- Reproducing the work of others without their permission or acknowledgement

7. Related Documents

As well as a full understanding of this document users should also check the following related documentation for relevance to their particular circumstances.

- Cyber-safe, Acceptable Use Guide for I.C.T @ TLC (P-4)
- Cyber-safe, Acceptable Use Guide for I.C.T @ TLC (5+)
- Cyber-safe, Acceptable Use Guide for I.C.T @ TLC (Staff)
- Cyber-safe, Acceptable Use Guide for I.C.T @ TLC (Visiting Staff)
- Mobile Phone Policy
- Student Laptop Program Guide