Clairvaux MacKillop College Acceptable Use of IT Policy

Purpose

The purpose of this Policy is to outline the requirements for regulating acceptable use of technology at Clairvaux MacKillop College. This policy establishes baselines and general principles for acceptable use of information, systems, networks and devices associated with Clairvaux MacKillop College, including their personal use.

The use of IT facilities is critical to enable Clairvaux MacKillop College to meet its learning and teaching objectives. However, if IT facilities are used in an unacceptable way, Clairvaux MacKillop College could be exposed to security threats and breach of legislative or regulatory requirements or suffer damage to its reputation.

This policy defines the acceptable use of the College's IT facilities to minimise the risk of a security incident resulting from the misuse of these facilities.

External Influences and Drivers

This policy is influenced by external factors including:

- Queensland Government Information Security Policy – Mandatory Clauses;
- Legal, Legislative and Privacy requirements;
- Regulatory requirements;
- Contractual obligations; and
- Industry good practices.

Enforcement and Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Brisbane Catholic Education reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Brisbane Catholic Education does not consider conduct in violation of this policy to be within any users scope of employment, enrolment or association with BCE. Accordingly, to the extent permitted by law, BCE reserves the right not to defend or pay any damages awarded against any user, including, but not limited to, employees, students or parents, that result from violation of this policy.

Any user who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, teacher, principal, any other manager or the Director Employee Services as soon as possible.

Any request for exceptions must be lodged with the Chief Information Officer (CIO) and managed through the IT Security Exceptions Register.

Definitions

- **Information** means any content that has value to the College. This includes information that belongs to the College; that is entrusted to the College in its role or information that is entrusted to the College as a service provider, and includes personal information of employees, students, parents/guardians.
- **Information security** means the preservation of confidentiality, integrity and availability of information assets.
- **IT** means Information Technology.
- **IT devices** means servers, desktop computers, mobile IT devices, facsimile machines, telephones, printers and any other electronic devices with the ability to process, store and/or transmit electronic data.
- **IT facilities** means information processing facilities including: IT devices, portable storage devices, IT systems, internet and email access and associated infrastructure and physical locations housing them.
- **Mobile IT device** means laptop and tablet computers, mobile and smartphones, media players and any other portable electronic devices with the ability to process, store and/or transmit electronic data.
- **Portable storage device** means USB flash drives, portable hard drives, memory cards/sticks, and any other portable devices with the ability to store electronic data, including electronic media, such as CDs, DVDs and other optical and magnetic media.
- **Software means** computer programs that enable an IT device to perform a function. These include applications ('apps') accessed indirectly through a web browser, and on social media and other web sites.
- **User means** any person that accesses or uses the College's information or technology facilities or equipment regardless of device, medium or location, including, but not limited to, its employees, students, parents, consultants, visitors, or any associated institutions users for which BCE provides information or technology services.

Policy Statements

Summary

- All College employees are responsible for information security;
- Users must use information technology in a responsible manner;
- Every user of College information assets must obey the law; relevant laws include but are not limited to the privacy, copyright, crimes, workplace surveillance, classification and spam acts;
- Information must be protected according to BCE's Data Classification Standard and Privacy Policy;
- Users must not install unauthorised equipment within the BCE network;
- Users must protect their College-provided portable equipment such as notebooks, tablets and smart phones from theft;
- Users must use virus protection and seek expert help in resolving virus problems;
- Users must report any security incidents and weaknesses according to Incident Management Policy;
- Users should use information technology for work related purposes and must not use College devices, facilities, networks or information for personal gain;
- The use of computer equipment and Internet access to accomplish job responsibilities will always have priority over personal use;
- Users of College information technology will be monitored by BCE as allowed legally;
- Users must not access or store illegal, offensive or inappropriate material;

General Conduct

- All users must use computing and information technology resources in a responsible manner.
- Each individual user has an obligation to abide by BCE and College policies and standards of acceptable and ethical use while using BCE and College equipment, facilities or systems.
- BCE and College services may not be used by any employee to engage in commercial activities for personal gain.
- Employees may not use BCE or College services to endorse any product or services.
- The use of computer equipment and Internet access to accomplish job responsibilities will always have priority over personal use. Access to services and facilities and information may be restricted at BCE's and the College's discretion.
- BCE reserves the right to monitor use of BCE's computer and information technology resources by each and every user. Any such monitoring is conducted in accordance with any relevant legal requirements.

Ethical Use

Users should observe ethical standards of conduct. Unethical activities may include:

- Granting access to unauthorised users;
- Attempting to, or successfully, modifying system facilities, illegally obtaining extra resources, degrading the performance of any system, or subverting the restrictions associated with any computer system, computer account or network service;
- Utilising access for commercial or personal gain not associated with College's mission;
- Obtaining or attempting to obtain a higher level of access privilege or access to facilities without authorisation;
- Using another person's computer account (even with the owner's permission, except in exceptional circumstances such as in an attempt to resolve an IT support incident for the owner);
- Disclosing their own or attempting to discover any other computer user's password;
- Denying access to other authorised users; and
- More than an incidental level of personal use of College devices, facilities, networks.
- Utilising any of College's information for personal use or professional gain.

Socially Responsible Use

- Users must ensure that their use of College's IT facilities is socially responsible.
- College IT facilities must not be used to humiliate, intimidate or offend others particularly on the basis of any attribute prescribed under these laws and policies. This includes the sending of offensive emails, displaying inappropriate screen saver images and accessing inappropriate material, which may inadvertently be observed by others.
- Commonwealth and State Laws and BCE policy prohibit harassment and discrimination, vilification or victimisation on grounds such as race, gender, religious belief, political conviction, sexual preference, or disability.
- Material that can cause offence such as pornography, hate, sexist, racist and other offensive material may not be accessed, held or displayed on any IT device, network or facility. Use, viewing, accessing or storage of obscene, illegal, undesirable or inappropriate material is prohibited. Additionally, any user found viewing illegal material will be referred to the police and their employment or enrolment may be terminated.

Legal Use

- BCE and College services may only be used for lawful purposes.
- Users must ensure their use of the BCE and College IT facilities complies with all relevant Federal and State legislation.
- Illegal activities include but are not limited to:
    - Intentional damage of IT facilities;
    - Breach of copyright;
    - Using College devices, networks or facilities for unauthorised access, interception, data interference or system interference to computers and networks is contrary to the Crimes Act 1914 (cth);
    - Theft of equipment, software or data;
    - Creation, possession or distribution of illegal pornography;
    - Unauthorised surveillance of employees;
    - Cyberstalking; and
    - Any other unlawful activity.
- Transmission, distribution, or storage of any information, data or material in violation of Australian or state regulations or laws, or the common law, is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret or any other statute. BCE reserves the right to audit and remove such illegal material from BCE's servers.
- Users must not breach any software license agreement or copyright, including copying or redistributing copyrighted computer software, data or reports.
- Users must not give the personal details of any person (employee, student, parent or other) to anyone unless you are sure that to do so will not be in breach of the Privacy Act 1988 (cth).
- If you use information created by someone else, you must
    a. have permission to use the material and
    b. always credit the owner or author.

  The important thing is to obtain permission to use the third party's material.
- The College requires that users must pay strict adherence to software vendors' license agreements and copyright holders' notices. Unless they receive information to the contrary, users should assume that software and other materials are copyrighted.

Professional Standards of Conduct

- Users of BCE's IT facilities must observe BCE's Code of Conduct. Unacceptable activities include:
    - Plagiarism;
    - Unauthorised publication on behalf of BCE; and
    - Unauthorised experimenting with or demonstrating of network or system vulnerability.

Competent Use

- Users should ensure that they are competent in the general use of communications, network and computing facilities and services. In particular users should:
    - Choose secure passwords and change them periodically;
    - Know how to back-up programs and data for which they are responsible;
    - Understand their responsibilities under BCE's Information Security Policy;
    - Assume responsibility for the maintenance and protection of data and software in their charge;
    - Take all practicable measures to ensure current local virus protection mechanisms are in place; and
    - Seek assistance if they do not know how to competently use the facilities.

Users' Responsibilities

All users must:

- Refrain from accessing or downloading information from BCE's or College's systems, unless those materials are required for performance of their job;
- Refrain from any practices that might jeopardise College computer systems and data files;
- Familiarise themselves with any special requirements for accessing, storing, protecting, and utilising information, including information covered by the Privacy Act 1988 (cth), copyrighted materials and commercial-in-confidence material; and
- Conduct themselves in a way that reflects positively on Clairvaux MacKillop College

Maintaining Confidentiality

- If in doubt, users should treat all non-public information as Restricted
- Sensitive information must not be disclosed to employees who do not have a business related "need to know".
- Disclosing passwords is prohibited. Passwords are personal and must never be disclosed or written down.

Systems & Network Use

Appropriate usage of Clairvaux MacKillop College systems and network is expected. As such, users must ensure that:

- Information, including student assessable material, must be stored on servers, which are backed up by the College.
- All users must run an approved virus protection software package on their computers;
- The College is responsible for installing and managing approved anti-virus software, which must not be disabled by a user;
- If a user transfers files between a computer in their home and a computer within the College network, that user is responsible for making certain that those files are scanned for viruses;
- Users must not attempt to eradicate viruses without expert assistance. If users suspect infection by a virus, they must immediately stop using the involved computer, disconnect from all networks, and seek expert assistance. If the suspected virus appears to be damaging information or software, users must immediately turn-off the computer;
- Users must not intentionally introduce malicious software (malware) to the College's networks. Examples of malware are viruses, worms or Trojan horses;
- Users must not attempt to circumvent access controls that have been put in place preventing their access to information. If a user is unable to access information that they require for their job, then they must obtain approval using the correct procedure to gain access. Access controls are put in place to preserve security. Users must not attempt to bypass these controls;
- Users must not extend the network in any way without authorisation. Users must not install any network device within the network without authorisation.
- Users must not attempt to circumvent user authentication measures or the security of any host, network or account;
- Users must not access data not intended for the user, log into a server or service with an account the user is not expressly authorised to access, or probe the security of networks or services;
- Users must not run security utilities that reveal weaknesses in security
- Users must not attempt to interfere with service to any user, host or network;
- Notebooks and tablets must be secured when left unattended; and
- In a vehicle, notebooks and tablets must be stored in a secure position. These devices should not be left in view or where they may suffer damage through falling. They should be locked in the car boot if it is necessary to leave them in a parked car.

The Use of Remote Access Facilities

- No remote access will be allowed without up to date virus protection and personal firewall software.

Reporting Security Incidents

- Users must promptly report all information security incidents including viruses, perceived weaknesses, suspicious activity, suspected vulnerabilities and any other security issues.
- Users must not forward such information to other users.
- Users who become aware of such behaviour taking place by any other user are mandatorily required to report such activity (Data Breach Notification)

Electronic Messaging Policy

- Electronic messaging is made available to the users as a tool to enable efficient performance of their daily tasks. However, the following requirements must be followed:
- All messages generated on or handled by the College electronic communication systems are considered the property of BCE;
- BCE is the owner of, and asserts copyright over, all electronic communications created by employees as part of their employment and sent through BCE's network. The only exception to this is where the copyright is owned by a third party;
- Electronic communications created, sent or received by the users of the BCE network are the property of BCE, and may be accessed as records of evidence in the case of an investigation. Electronic communications may also be subject to discovery in litigation and criminal investigations. Email messages can be retrieved from backup systems and organisations, employees and the authors of email are liable for email messages that have been sent;
- BCE electronic communications systems generally must be used for educational purposes only. Incidental personal use is permissible provided it does not pre-empt any business activity;
- News feeds, email mailing lists, push data updates and other mechanisms for receiving information over the Internet must be restricted to material which is clearly related to the duties of the users;
- Electronic mail systems must employ personal accounts and associated passwords to isolate the communications of different users;
- Users must not employ the user-ID or other identifier of any other user. Misrepresenting, obscuring, suppressing or replacing another user's identity on an electronic communications system is strictly forbidden;
- The user name, electronic mail address, organisational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings;
- Users must not use encryption for any production electronic communications system unless a backup key or a key escrow system has been established;
- Users are reminded that not all of BCE's electronic communications systems are encrypted by default. If sensitive information must be sent by electronic communication systems, encryption or similar technologies to protect the information must be employed;
- Except where authorised by management acting in compliance with relevant legislation, users may not intercept or assist in intercepting or disclosing, electronic communications;
- BCE is committed to respecting the rights of its users, including their reasonable expectation of privacy;
- Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, people other than the intended recipients can access electronic communications;
- Because messages can be stored in backups, electronic communications may be retrievable after deletion from a user's mailbox;

- All BCE electronic communications must be consistent with conventional standards of ethical and polite conduct. Users must not use profanity, obscenities or derogatory remarks in electronic mail messages. Such remarks may create legal problems such as defamation;
- All attachments will be scanned for viruses and unsuitable content and if any are found the attachment will be deleted. Attachments to electronic mail messages may contain a virus or may in some other way damage a user's computer. All attachment files must be scanned with an authorised virus detection software package before opening and/or execution. Unexpected attachments received from third parties should be viewed with suspicion. Even if the third party is known and trusted, viruses may still cause an infected attachment to be sent;
- College sensitive information must not be forwarded to any party outside the College
- Recognising that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages;
- Blanket forwarding of messages to parties outside BCE is prohibited;
- Messages sent by outside parties should not be forwarded to other third parties unless the sender clearly intended this and unless such forwarding is necessary to accomplish an ordinary business objective;
- In all other cases, forwarding of messages sent by outsiders to other third parties can only be done if the sender expressly agrees to this forwarding;
- Electronic messages that constitute records must be retained. If an electronic mail message contains information potentially important reference information or has value as evidence it must be retained for future reference.
- Harassment or bullying using College equipment or systems is strictly prohibited and is cause for disciplinary action up to and including termination;
- Users who receive offensive unsolicited material from outside sources must not forward/redistribute it to either internal or external parties.
- Transmitting on or through any of BCE's systems, services, or products any material that is, or may be deemed to be, unlawful, obscene, pornographic, threatening, abusive, defamatory, or hateful, is or encourages conduct that may constitute a criminal offence, may give rise to civil or any other liability, or otherwise may violate any local, state, national or international law, is prohibited; and
- The above provisions apply to all electronic messages, whether sent by email or any other means of messaging using BCE computing and information technology resources.

Passwords

Construction

Users must choose strong passwords. Poor, weak passwords have the following characteristics:

- The password contains less than eight characters;
- The password is a word found in the dictionary;
- Names of pets, family members, partners, colleagues, etc.;
- Computer terms and names, commands, sites, companies, hardware, software;
- Derivatives of the company name;
- Birthdays and other personal information such as addresses, phone-numbers, employee codes, etc.;
- Profanity, obscene language or sexual innuendo;
- Word or number patterns such as aaabbb, qwerty, 123321, etc.;
- Any of the above spelled backwards; and
- Any of the above preceded or followed by a digit, e.g. Fiona1, 3Tuesday, etc.

Strong passwords have the following characteristics:

- Contain both UPPER and lower case letters;
- Contain both alpha and numeric characters as well as having punctuation characters, e.g. 0-9, !@#$%^&*()_+~`, etc.;
- Are at least eight characters long;
- Are not a word in any dictionary, jargon, slang, dialect; and
- Are not based on any personal information.

Password Protection Standards

The following rules must be followed to protect passwords:

- Do not reveal passwords to anyone telephonically or electronically;
- Do not use the same password for corporate and personal access accounts;
- Do not reveal your passwords to support people or superiors;
- Do not talk about passwords in front of others;
- Do not hint at the format of your passwords;
- Do not share passwords with family members;
- Do not reveal passwords to co-workers while you are out of the office or school for extended periods of time;
- Do not share passwords with any co-workers, e.g. administrative secretaries; and
- Do not write down your password.

Internet Access

- Internet access is controlled through individual network accounts and passwords. Incidental personal use is permitted but must not affect your work, other users or the system performance.

Inappropriate Use

- Individual Internet use should not interfere with others' use of the Internet. Internet use at Clairvaux MacKillop College must comply with all Federal and State laws, all company policies, and all company contracts. This includes, but is not limited to, the following.
    - The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, defamation, fraud, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering;
    - The Internet may not be used to view, download or distribute pornographic, illegal or offensive material; and
    - The Internet may not be used in any way that violates BCE or College policies. Use of the Internet in a manner that misrepresents or violates any policy is prohibited.
- In the interest of maintaining network performance, users must not send or download any large file, such as: graphics, videos or music, unless required for business use or agreed by management. Similarly, users must not stream non work-related content, such as radio or television programs from the Internet.
- BCE or the College is not responsible for the content that users may encounter when they use the Internet. When and if users make a connection with web sites containing objectionable content, they must promptly move to another site or terminate their session.
- Users of BCE information systems or the Internet must realise that their communications are not automatically protected from viewing by third parties. Unless encryption is used, users must not send information over the Internet if they consider it to be confidential or sensitive.
- The College is not responsible for material viewed, downloaded, delivered or received by users through the Internet. Employees are solely responsible for any material that they access and disseminate through the Internet.

Monitoring

- Electronic communications, devices, networks and facilities are monitored by BCE and CMC Connect.
- From time to time BCE may examine the records of electronic communications including for operational, maintenance, compliance, auditing, security or investigative purposes. Monitoring may occur of web sites visited. The contents of email may be required by law to be disclosed. BCE may need to check email in a user's absence for business reasons, or BCE may need to investigate a complaint arising from the use of email or other electronic communications.
- Electronic Communications are provided to you on condition that you agree to monitoring in accordance with this policy and the law. Your use of electronic communications constitutes your consent to monitoring in accordance with this policy.

References

Acceptable Use (bne.catholic.edu.au)
Privacy Statement (bne.catholic.edu.au)
Information Security policy (sharepoint.com)