122 Information and Communications Technology Policy

Purpose

1. To provide clear guidelines on the use of the Community College GippslandCCG) Information and Communications Technology (ICT) facilities.

Policy

2. CCG operates from multiple campuses across a wide geographic region with a corresponding range of staff from full time through to sessional staff. The provision of appropriate ICT facilities to enable effective educational delivery, comprehensive staff communications, and on-going management of our business is critical to CCG's financial viability and future success.

3. CCG provides and maintains its ICT facilities for CCG business use. It recognises that some limited personal use may be permitted from time to time. Any personal use must be minimised and may be monitored. Excessive personal use will be reported and staff may be required to reimburse CCG for such use.

4. ICT equipment and other resources issued to staff remains the property of CCG – this includes intangibles such as mobile phone numbers and the like.

5. The allocation of appropriate ICT equipment is a management decision and instances of inappropriate use may see access withdrawn or disciplinary action taken.

6. CCG allocated Mobile Phones are to be used for business purposes only, no personal use is permitted.

Scope

7. This policy, including standards and regulations, applies to:

   - All CCG staff.
   - All CCG students.
   - All CCG ICT resources. For the avoidance of doubt this includes computers (desktop and laptop) and ancillary devices such as displays; tablets; printers, copiers and scanners; data projectors; mobile phones; wireless broadband modems; servers; intranet; internet; email; cable network; wireless network and other equipment as identified from time to time.

Responsibilities

8. The Chief Executive Officers and Directors are responsible for the operation and review of this Policy in accordance with general 'good practise'.

Definitions

CCG Business Use:	Use for the conduct of business associated with the delivery of administrative functions and courses for students and other operations associated solely with CCG.
Inappropriate Use:	Excessive personal use OR use that involves objectionable or illicit material OR use for external or other non CCG business purposes.
Personal Use:	Anything other than CCG business use. This includes all use for social media such as Facebook, Twitter or equivalents; on-line shopping or auctions; personal telephone calls and texts; and any usage that may arise from time to time that is not directly associated with conducting business for CCG.
User or Users:	All staff, contractors and students utilising CCG ICT resources

Relationships

Internal:

Policy 423 Code of Conduct and Disciplinary Procedures
Policy 411 Bullying Harassment and Discrimination Policy

External:

Procedures

When communicating with IT Services staff, email itsupport@ccg.asn.au in the first instance or telephone for more urgent matters.

Forms

Nil

APPENDIX

a. ICT Standards and Regulations

b. Mobile Devices

ICT Standards and Regulations

Standards

Acceptable Use

1. Community College Gippsland's (CCG) ICT environment is dynamic and provides for effective sharing, transport and storage of information and communications for educational delivery and the operation of the business. This standard will respect this environment and inhibit these characteristics only when necessary to protect the essential interests of CCG.

2. ICT resources, including internet, telephony, messaging and email services, are provided for the purposes of conducting CCG business. It is acknowledged that limited personal use will occur and is acceptable. "Limited personal use" means private use that is infrequent and brief. Personal use may be monitored and reported to Managers as required. Instances of on-going use beyond limited personal use may require reimbursement of costs by the user to CCG and or lead to disciplinary action being taken. CCG accepts no liability for any loss or damages suffered by users as a result of personal use.

Access

3. Academic and administrative staff will be authorised to access resources required to perform their duties.

4. Students will be authorised to access services for academic purposes relating to their course of study.

Privacy

5. CCG recognises the right to privacy of staff and student files and communications in accordance with Policy 131 Information Privacy. However, CCG reserves the right to examine files and directories where it is necessary to determine the ownership or recipient of lost or misdirected files, and also where CCG reasonably believes that:

   a. System integrity is threatened,

   b. Security is compromised,

   c. An activity has a detrimental impact on the quality of service to other users,

   d. The system is being used for purposes which are prohibited under this standard, or

   e. The system is being used for unlawful purposes

6. You should exercise caution when storing or transmitting any confidential information in electronic format, because the privacy of such information cannot be guaranteed.

Network Integrity

7. The CCG network is recognised as a key element of the ICT services that support the delivery of courses, the administration and storage of records, and the management of the business.

8. Systems and users are registered and allocated an appropriate network address which is compatible with all other equipment and systems associated with the network.

9. Any form of alteration or manipulation of the CCG network is prohibited.

Standard Computing Environment

10. A standard suite of office applications and essential software is adopted in order to maximise benefits to the CCG community in the form of improved communications, reduced resource usage, greater productivity and lower technical support requirements for users.

11. Software required beyond this standard may be installed only with the permission of the IT Services Manager and will be classified as 'non-maintained' applications.

Defamation, Harassment and Other Abusive Behaviour

12. No user will, under any circumstances take any action which would or might lead to CCG's ICT facilities being used for the purpose of defaming or slandering any individual or organisation. The ICT facilities must not be used in any way such that a reasonable individual may consider this action to be viewed as harassing, abusive or obscene behaviour (see also Social Media)

Objectionable or Illicit Material

13. No user will, under any circumstances use CCG's ICT facilities to access, transfer, or store objectionable or illicit material.

Copyright

14. The Copyright Act sets out the exclusive rights of copyright owners and is intended to provide protection for the intellectual property of those people who have created something original, as well as specifying the rights of users.

15. If you use an image, sound, or video in a presentation, copy material produced by another person, use text written by someone else in a document, or make a copy of a computer program, you may be infringing copyright.

16. The Australian Copyright Act 1968 and the Australian Copyright Amendment Act 1984 provide strong legal protection against unauthorised copying or use of computer software with heavy penalties that apply to individuals and organisations that breach the Act. In brief, it is illegal:

    - To copy or distribute software or any accompanying material without the permission or licence from the copyright owner;
    - To run a software program on more than one computer simultaneously unless the licence agreement specifically allows this;
    - For any user at CCG to consciously encourage or request any staff member to make, use, or distribute illegal software copies;
    - To copy protected software because a superior, colleague, or friend requests or compels it;
    - To loan software so that a copy can be made, or to copy software while it is on loan.

Knowledge of Breach of Standard

17. Should any user become aware of any action by another individual which could be considered to breach any part of this Standard, they are requested to bring it to the attention of the IT Services Manager.

Disciplinary Action

18. Disciplinary action arising from misuse of CCG ICT facilities will be taken in accordance with Policy 423 Code of Conduct and Disciplinary Procedures

Social Media

19. Social media is a term used to describe web-based media that is used for social interaction that includes networking, blogs, wikis, and other such tools.

20. CCG uses social media for marketing and PR purposes. The Directors Executive Assistant and Marketing Coordinator (DEAMC) has full responsibility for CCG's social media sites. Any other requests to use social media for CCG business purposes are to be directed your manager for approval.

21. Reasonable personal use of social media is permitted during work breaks only so as not to affect operational requirements.

22. CCG respects an individuals right to use social media for personal communication and self expression. However, caution should be exercised in using social media and all users should be aware that making comments or conducting conversations that relate to CCG's business, staff, students or clients can affect our reputation and business.

23. The following use of social media is not acceptable and may lead to disciplinary procedures:

    a. Any behaviour that identifies the business, staff, students, or clients in a disparaging or unacceptable way whether it is inside or outside of the CCG environment and regardless of whether it is on personal or CCG devices.
    b. Any actions that has the potential to bring CCG into disrepute
    c. Any actions that gives away CCG's business information or intellectual property
    d. Any actions that could be viewed as derogatory towards or disparaging of staff, students, or clients
    e. Any actions that could discriminate, harass, bully, or victimise any person
    f. Undermines staff effectiveness or productivity at work through excessive use
    g. Cyber Bullying or harassment in any form

Regulations

Acceptable Use

1. Unauthorised use of any CCG ICT facility is not permitted. Those who make use of the CCG ICT facilities are required to behave in a manner consistent with CCG's Policies and Codes of Conduct including these Standards and Regulations. As a user of these resources, you agree to the following usage regulations:

    a. You are responsible for the use of any computer account you have been given. You shall set and use a password on the account that is not easily guessed and you shall not share this password with any other person.

    b. If you discover that someone has made unauthorised use of your account, you should immediately change your password and report the event to IT Services staff.

    c. Any breach in system or network security should be reported immediately to IT Services staff.

    d. Electronic mail and online postings should be treated as if they were tangible documents. Staff members are reminded to distinguish between personal opinion and authorised CCG statements when communicating electronically or online and should ensure that no addressee can infer that your personal opinions are necessarily shared or authorised by CCG. In these circumstances, it is a staff member's obligation to clearly identify them as their opinions and not those of CCG.

    e. CCG's ICT network, internet provision and disk storage are not unlimited resources. Quotas for storage and internet use should be observed, to ensure that associated usage costs are sustainable.

Authorised Users

2. Access to the CCG ICT facilities is for authorised staff, students, and other users as may be approved from time to time subject to appropriate authorisation and indemnities.

3. Users are responsible for the use of their own accounts and are permitted to access only those resources for which they have been authorised. No user may use any other user's authorisation to access any system or allow any other person to use their authorisation to access any system.

4. There may be a limited number of 'non-user' accounts set up for general access within a Department as approved by the IT Manager from time to time.

Registration of Users

5. Users are provided with system access as part of their induction process by IT Services staff . Requests for new user accounts are normally contained in the New Employee Notification form and are to be lodged with IT Services staff prior to the employee starting work with CCG.

6. All academic and general staff must be authorised by their delegated manager to access ICT Facilities that are identified as being required to perform their duties.

Cancellation of Registration

7. User access will be disabled on the last day of employment or when the access is no longer required to perform their duties.

8. Any user may have their access terminated or suspended for breach of any of the terms of this standard or related standards, as determined by the IT Services Manager and the user's Manager.

Security

9. A primary means of security for CCG's ICT facilities is through the allocation of individual computer accounts and access passwords. It is every user's responsibility to ensure that:

    - Passwords are selected carefully and not shared with other persons,
    - Computer equipment is kept physically secure, and
    - Computer accounts are not shared with other persons.

10. No user will, under any circumstances, take any action which would or might lead to circumventing or compromising security of any of CCG's ICT facilities.

11. A user should use any available methods to safeguard data, including regular changes of passwords, ensuring files are stored on CCG networks in approved locations requesting secured storage for sensitive data and encrypting or protecting sensitive data that is sent or taken off premises. In the event that your files have been corrupted or compromised, you must notify IT Services staff immediately.

12. You are advised that computer systems and the Internet are not completely secure. It is possible that others will be able to access files by exploiting shortcomings in the system security. For this and other reasons, CCG cannot assure confidentiality of files and other transmissions.

13. The IT Services Department attempts to provide reasonable security against damage or loss to files stored on CCG's equipment by making regular backups. In the event of lost or damaged files, a reasonable attempt will be made to recover the information. However, CCG and IT Services staff cannot guarantee recovery of the data.

14. All computers should be secured by logging off when the equipment will be unattended. They should also be set to do this automatically if unattended for a period of no more than 15 minutes.

15. Information contained on mobile computing equipment such as laptops and tablets is especially vulnerable and special care should be exercised. Where mobile computing equipment is not taken home after hours, CCG users are responsible for ensuring that this equipment is secured in a locked room or container.

Use of CCG Property

16. Community College Gippsland's ICT facilities, as with other CCG resources, are not to be used for purposes other than those deemed appropriate by CCG as defined in CCG Policy. It is recognised that limited personal use will occur and cannot be totally eliminated. Excessive personal use (such as storing large numbers of personal photographs or videos) is not appropriate.

17. On the whole it is expected that staff will not use CCG's ICT facilities for private purposes and students may not use CCG's ICT facilities for purposes other than those directly related to their studies.

Official Representation of CCG

18. Users must be aware that the correspondence and discussion into which they enter when using the CCG network and the Internet may be construed to be representative of CCG's position.

19. Where the user is representing the views of CCG, then a notation or 'signature' must be appended to the communication identifying the individual and the position title held within CCG.

Expression of Personal Views

20. Where the user does not have authority or is not aware of CCG's position or where their personal view may vary from that of CCG, such correspondence must clearly state that the opinion expressed is that of the writer, and not necessarily that of CCG, or words to that effect. For the avoidance of doubt, this includes comments made on social media sites.

Electronic Communications and Online Content

21. Facilities for electronic communications (such as electronic mail, blogs, wikis, list servers and news) are provided for general use consistent with this and other CCG policies.

Interference to or Monitoring of Other Users

22. No user will, under any circumstances, take any action which would or might lead to denial of service or impairment of access to or effective use of, any ICT resource by any other authorised user.

23. No user will, under any circumstances, take any action to monitor the network or segments of the network in order to intercept the communications being sent to or from a user on the CCG network unless such monitoring is authorised.

24. The propagation of software viruses, malware or similar contaminant software is expressly forbidden.

Malware (Viruses and Spyware)

25. Users need to consider all of the possible points of malware entry (internet, email, removable media, personal computers, gateways, servers, staff computers connected by modems) when addressing the potential risks, and implement appropriate actions to counter those risks.

26. The success of any actions implemented depends on the detection products used and the regular use and updating of these products. As a consequence, it is imperative that you adopt a malware protection strategy and rigorously adhere to it.

27. The following guidelines are provided to assist you in implementing a successful malware protection and detection strategy. Remember that the ease with which malware can be introduced onto your computer will depend on your ability to implement these simple steps.

    - Scan your computer regularly for malware using the supplied virus detection software. This check should be performed at least every week

- Identify any possible virus intrusion points where malware is more likely to enter your equipment. Implement more stringent protection measures in these areas.
- Scan any removable media when inserted.
- Electronic mail messages and web sites may contain viruses and malware. Scan attachments or downloaded files prior to using them on your computer.
- Never click on links or attachments in unsolicited email or messages of dubious origin. If in doubt, seek confirmation from the sender.

28. If you suspect that your computer may be infected by malware, contact IT Support staff immediately so that measures can be taken to remove the malware and identify any other affected computers and storage media.

Reporting Faults, Issues and Missing Equipment

29. Faulty or damaged equipment and any theft or loss must be reported as soon as possible to IT Services staff.

Mobile Devices

Mobile Devices

1. Users need to be aware of the specific risks that apply regarding the use of mobile devices. The following guidelines are provided to assist users to comply with good practice.

    - Personal computers should not be used at home for business activities if virus controls are not in place.
    - When travelling, ICT equipment and media should not be left unattended in public places. Portable computers should be carried as hand luggage when travelling.
    - Time-out password protection should be applied.
    - Portable and attractive items such as portable computers, tablets, mobile phones, PDAs and digital cameras are vulnerable to theft, loss or unauthorised access when travelling. They should be provided with an appropriate form of access protection (eg. Passwords and/or encryption) to prevent unauthorised access to their contents.
    - Passwords or other tokens for access to CCG's ICT systems should never be stored on mobile devices where they may be stolen, allowing a thief unauthorised access to information assets.
    - Manufacturer's instructions regarding the protection of equipment and data should be observed at all times.
    - Security risks (eg. of damage, theft) may vary considerably between locations and this should be taken into account when determining the most appropriate security measures.

Responsibility

2. Employees are responsible for the proper use, care and maintenance of a CCG issued mobile phone or device, and must:

    - not use the phone or device for any unlawful activity, personal financial gain, or for commercial purposes not authorised by or under the auspices of Community College Gippsland;
    - not use a CCG mobile phone for personal use
    - report any faults or damage to phones or devices and any theft or loss immediately to the Finance Manager? in order for a replacement to be ordered and the service provider to be notified;
    - not use the phone or device whilst driving unless via a properly fitted Bluetooth or hands free device. No part of the phone or device is to be touched whilst driving.
    - pay any fine incurred as a result of illegally using the phone or device when driving; and
    - return the phone or device in good working order on cessation of the need for their position to have the phone or device or of their employment with Community College Gippsland. If the equipment is not returned in good order the cost of necessary repair or replacement may be deducted from outstanding benefits or entitlements that the employee has under their contract of employment.

Types of mobile phone or device issued

3. CCG will issue mobile phones or other telecommunication devices to employees as are deemed by management to be necessary for proper performance of their roles. The type and features of the phone or device will be commensurate with the job the employee is to do and will be determined by their Manager. Accessories may include a vehicle charger, an AC charger, and a protective case as appropriate and available.

Efficient use of mobile phones and other devices

4. CCG mobile phone are to be used strictly for business purposes only. The Managers will determine whether the phone issued should have the facility to access emails or calendars.

5. To reduce the costs associated with the use of company provided mobile phones or devices each employee must:

   - only use the mobile phone if an office phone is not available or when calling another CCG mobile phone;
   - be clear about what needs to be discussed before making a call, keeping the call as brief as possible and to the point. Mobile phones are usually billed in 30 second blocks. Calls from mobile phones are generally 3 to 5 times more expensive than calls from land line phones.
   - not forward or divert calls from the work mobile phone to a private mobile phone. Note that service providers charge for calls forwarded from mobile phones and it is more cost effective to use the mobile phone's voice mail facility; and
   - not use internet or social communications on the phone or device unless authorised to do so by their Manager and appropriate structures are in place by the service provider.

6. All users must accept full responsibility for using their company phone in an honest, ethical, safe and legal manner and with regard to the rights and sensitivities of other people. Use must be in accordance with company policies and all relevant Federal and State legislation.

Safe use of mobile phones

7. Employees issued with a mobile phone or other telecommunication device must read the manufacturer's manual provided and comply with the safety recommendations.

8. Mobile phones are not to be used when driving CCG vehicles unless in a fully ‘hands-free’ mode in accordance with Policy 621 Vehicles and Travel.

Electromagnetic radiation

9. CCG is aware of concerns in the community about allegations and claims of adverse health effects associated with using hand-held mobile devices including mobile phones. For updates on this issue employees should refer to the information bulletin on the website: www.arpansa.gov.au/is_phone.htm. The Australian Radiation Protection Safety Agency (ARPANSA) regularly updates this bulletin.