Bass Coast
Adult Learning
Learn More.

Policy 12 IT Security Policy

Version Number: 1.5

Relevant to all employees, volunteers and contractors of BCAL, this policy covers all areas of information security and use of information & communication technology.

Contents

1. Purpose

The purpose of this policy is to ensure that appropriate measures are put in place to protect students, staff, volunteers, contractors and corporate information and the Information Technology Services (IT) systems, services, and equipment of BCAL and associated infrastructure.

2. Objectives

The objectives of the Information Security Policy are:

To ensure the online safety of all BCAL students, particularly children and vulnerable students, staff, volunteers and contractors.

To secure BCAL assets against theft, fraud, malicious or accidental damage, breach of privacy or confidentiality; and

To protect BCAL from damage or liability arising from the use of IT facilities for purposes contrary to BCAL's Acceptable Use Agreements.

3. Scope

This policy applies to all BCAL staff, and any other persons otherwise affiliated but not employed by BCAL, who may utilise the IT infrastructure and/or access applications with respect to the security and privacy of information.

4. Definitions

Term	Description
BCAL	Bass Coast Adult Learning Inc.
Centre	Physical facilities (buildings and grounds)
Google Workspace for Education	A suite of online serves including Gmail, Google Drive, and a range of additional online applications.
Drive	Google Drive is a cloud storage and sharing service. This is the primary used by BCAL for storage and access to most of BCAL documents.
Vault	Google Vault is an information governance and eDiscovery tool for Google Workspace. With Vault, you can retain, hold, search, and export users' Google Workspace data. Vault allows delegated offices to review user activity across a range of applications such as Google Drive and Gmail.
Google Administrators	Accounts that belong to this Admin Group have control over the accounts and resources that users can or cannot access. This

Term	Description
	group of users are responsible for dealing with any security and data integrity issues.
VETtrak	VETtrak is a Student Management System used for RTO compliance. BCAL uses this system for is enrolment and course information and reports this information to the respective educational authorities.
Trainer Portal (VETtrak)	This online application is used by trainers to record attendance, results, and to communicate to students via SMS or email
WAP	Wireless Access Point – Provides wireless signal that can but used be end users to connect to the Internet.
Router	Manages income and outgoing traffic between the local network and the internet. The router can also act as part of a filtering of content.
Google – Age Restrictions	This is a filtering feature that applies to secondary or underage students. This restricts the types of online portal that student can interact with.
Incident	An occurrence of inappropriate or suspect activity that may be illegal or not with within BCAL Acceptable Use Policy.
User ID	Login details assigned to a user to enable them to use the ICT facilities.
VPN	Virtual Private Network. A secure connection between to two locations on the Internet.

5. Policy Statement

The Information Security Policy determines how the IT services and infrastructure should be used in accordance with IT industry standards and to comply with strict audit requirements.

6. Staff Access

BCAL provides staff with access to computing and communications services in support of IT business activities. These facilities include access to email, Internet, file and print services, an integrated data network, and Service Desk.

Users are responsible for maintaining the use and security of their assigned User IDs and all activity associated with that ID. Knowingly disclosing passwords to others will be deemed a breach of policy and could be referred to disciplinary procedures.

BCAL expects IT staff and associates to take all reasonable steps to ensure the integrity and security of IT systems and data.

7. Human Resources Responsibilities

It is the responsibility of Human Resources to ensure correct termination dates are entered into the HR system for staff terminations. After a fixed number of days from the date of termination, the

staff account will be disabled. Following a further pre-determined number of days, the account will be deleted.

There are situations where an account may need to be disabled immediately and this can only be performed with the authorisation from BCAL's Executive Officer or delegated officer.

Contract / Temporary Access

Where temporary access is required for a specific purpose such as, but not restricted to, contract workers and 'test' accounts, a user expiry date based on the completion date of the required tasks must be used to ensure the temporary account is not accessible after that date.

In the case of ongoing maintenance and support from 3rd party companies, access must only be granted to the relevant facilities within the system and be restricted to only the systems for which they provide support.

Reliance on People

All specialised computing staff are required to ensure that all systems and procedures are well documented and that there are others who can act in a backup capacity as required.

Staff Responsibilities

It is the responsibility of staff to be familiar with Information Security Policies and the Acceptable Use Agreements.

8. Acceptable Usage

Identification of what is deemed acceptable (or unacceptable) usage of network, communication, and Internet services.

9. Network Usage

BCAL provides staff with access to computing and communications services in support of IT business activities.

By signing the appropriate forms for obtaining access to the computing facilities, users agree to abide by all policies that relate specifically to the use of these facilities. Any breach of these policies will be deemed an infringement and dealt with accordingly which could result in suspension of access privileges or in severe cases, legal authorities will be involved.

Interfering, in any way, with the network or associated equipment, be it intentional or accidental, is not permitted. Any such interference will be acted upon and may result in removal from the network until an investigation can be completed and the source of the interference is removed.

9. Electronic Communications

BCAL encourages staff to appropriately use electronic communication in order to achieve the mission and goals of the business. BCAL encourages the use of electronic communication to share information, to improve communication and to exchange ideas.

The electronic communications services must not be used for the distribution of material that may be deemed offensive, discriminatory, or defamatory or the publishing or advertising of personal events or activities.

10. Internet Usage

BCAL encourages staff to use the internet in order to further the strategic and operational objectives of the business. BCAL encourages the use of the Internet to share information, to improve communication and to exchange ideas.

Inappropriate usage of Internet facilities includes, but is not restricted to, accessing or posting of discriminatory, defamatory, offensive material or material that may create or promulgate a negative impression of the business.

Any staff required, as part of their job function, to access information on the Internet that may be deemed inappropriate, must obtain written authorisation from the EO with a copy submitted to the Manager, IT Security and Risk.

11. Mobile Devices

Mobiles devices including, but not limited to, laptop and netbook computers, mobile phones, smart phones and tablet devices, are all subject to the same policies and procedures as for other computing and communication devices.

12. Security

Logical Security

Implementing a suitable environment that protects the integrity, availability, and confidentiality of BCAL data by using logical or 'computerised' controls and processes.

Software Security

Software security specifically relates to access rights and protection of software packages supplied by, and for the use by, BCAL computer services infrastructure. All staff are supplied with a User Account for authentication and allocation of appropriate access rights to network facilities including software. Access to such network facilities and software is also controlled using secure passwords which must be changed on a regular basis.

End-Point Security and Antivirus Software

All BCAL PCs and laptops have end-point security software installed which has an automatic pattern update feature enabled. This is to ensure that the software is kept updated for the latest threats.

There are also antivirus systems in place checking all incoming email into the organisation and on internally circulating emails.

It is expected that any non-BCAL PCs and / or laptops also have current updated antivirus software installed, and it's the owners / user's responsibility to ensure this. Not having current updated antivirus software installed exposes BCAL systems and infrastructure to potentially significant disruption and damage due to virus infected computers.

Passwords

It is essential that those requiring access to BCAL computing facilities be issued with a unique login and password. This password is not to be shared with, or used by, any other individual and failing to comply will be treated as a serious breach of system security which may result in disciplinary action.

Staff Passwords are to meet complexity rules. These complexity rules will include a minimum password length, character requirements and suitable password expiry period.

If access is required to data that is held under a specific staff members user id and password and that staff member is unavailable to access the data due to unforeseen circumstances, a request to have the password reset may be made with the authorisation of the delegated officer. This will only be considered when all other avenues to access the data have been exhausted. At the completion of the task accessing the required data, the password MUST be reset again, and the staff member notified as soon as is practical.

13. Data Security

Ensuring that the confidentiality of data contained on the information technology systems is maintained and access is made available to those who are authorised to see that data. This item should also be used in conjunction with confidentiality polices.

Confidential Data Security

To ensure the confidentiality and security of staff personal information contained on the IT facilities, it is essential that only those authorised to access such data are permitted to do so. Those who are permitted to access such information are granted appropriate access, as required by their job functions, by IT.

Anyone who gains access to such personal information through methods other than those granted by IT, shall be deemed as unauthorised and subject to disciplinary action.

Staff should be aware of their legal and corporate responsibilities in relation to appropriate use, sharing or releasing of information to another party. Any other party receiving restricted information must be authorised to do so and that the receivers of the data also adopt information security measures to ensure the safety and integrity of the data.

Communications Security

Communications between staff can use a variety of technologies. However, when using electronic communication staff are encouraged to use the BCAL accounts and not use their private account.

Staff may use mobile devices to communicate with other staff is necessary and where the other staff member has agreed to contacting them on their private phone number.

However, staff are not to use their private phone or email to contact students. Where students do need to be contacted via their private phone or email staff should use the Trainer Portal for SMS messages.

Physical Security

Ensure that the physical IT devices are kept safe from inappropriate access. This includes the physical access to the switch and patch panel cabinets, and any other IT devices in both restricted and public access areas.
Physical Access Security

All offices, computer rooms and work areas containing confidential information, or access to confidential information must be physically protected. This means that during working hours, the area must be supervised, so that the information is not left unattended, and after hours, the area must be locked, or the information locked away.

It is a requirement that any PC / Laptop / Portable computer be logged out and turned off at the end of the working day unless a specific request is made to leave equipment turned on for the purpose of distribution of overnight processing is required.

Building Access

The following controls must be applied to restrict building access:

a. Access to computer work areas must be restricted.
d. When unattended and after hours, doors must be secured, and security alarms activated.

Other workers must not attempt to enter restricted areas in BCAL buildings for which they have not received access authorisation.

14. IT Asset Control

All IT devices over a specified value must be registered with BCAL asset register. This also applies to the disposal of assets.

IT Asset Disposal

When disposing of IT assets such as computers, laptops, printers etc, the disposal must be co-ordinated with IT Service Support to ensure that all data is removed using approved security techniques.

Removal of Equipment

No computer equipment can be removed from BCAL premises unless specific authorisation has been received by the delegate officer. This does not apply to laptop or notebook computers where one of their primary purposes is to allow the custodian to work while away from their normal working location.

15. Mobile / Portable and Handheld Devices

Specific issues relating to resources such as, but not limited to, iPhone, Smart Phones, PDAs, iPad, mobile phones, laptop or notebook computers and the like and their use within the general system infrastructure.

Allowing Access

Since portable and handheld devices are more and more common, it is necessary that we allow for their use on the network. All new staff laptops will be passed via the Information Technology Services, or designated technical staff, for initial setup and testing to ensure that all the correct anti-virus and patch updates are installed and can be used safely on the network.

Accepted Usage

It is expected that the custodians of laptops or other portable device will still abide by this policy and all supporting documents. Any breaches of this policy may lead to disciplinary action being taken.

16. Security Incident Management

Specify how any breaches of security relating to the information systems will be identified and handled.

Reporting Security Problems

Any suspected inappropriate or illegal usage of BCAL Information services network and equipment should be reported to the Service Desk immediately. This information will then be reported to the Manager, IT Support for investigation.

Emergency Plans

Disaster Recovery Plans, Business Continuity Plans, backup strategies and fail over plans for the core IT Services and infrastructure are the responsibility of IT Services to ensure that any outages or disasters can be recovered from in the shortest possible time with a minimal amount of data or resource loss.

Escalation

The escalation process for the rating of each reported event will be determined by the relevant IT staff member in conjunction with IT Security considering the event and other priorities at that time.

Monitoring and Reporting

Staff nominated by the EO will be authorised to monitor all aspects of BCAL network and associated infrastructure. They are also able to report any suspected inappropriate and / or illegal activity to the IT Security and Risk Manager in the first instance for further investigation.

It is also the role of the IT Security team to actively monitor and analyse all network related activity included, but not restricted to, internet usage, email and dissemination and use of programs and data across BCAL network infrastructure.

This monitoring will be done for the sole purpose of identifying and responding to any suspected inappropriate activity.

The Student Management System VETtrak is hosted remotely and is frequently backed up. Any software update for VETtrak is dealt with remotely by the software developer. To access the SMS a VPN is used by a restricted number of administrative staff.

The content of e-mail and other electronic communications will only be accessed by the IT Security team-

- after approval has been obtained from the EO; and
- if the access is permitted by law.

All information reported to the BCAL's Security Team shall be treated in the strictest confidence. Any reported information will be logged, and relevant action taken, including reporting to relevant management as required.

17. Business Continuity

How to ensure that there will be minimal disruption to IT services in the event of a disaster or the implementation of changes to systems and/or associated infrastructure.

Backup Requirements

Most major systems within BCAL utilise Google Works Space for Education. It is also strongly advised that all users save their work to Google Drive. Ideally their work should be backed up are backed up and any loss or damage to files can often be rectified by the restoration of the files from an existing backup.

Disaster Recovery Plans

In the event of a disaster that impacts the IT infrastructure and / or services, the implementation of a Disaster Recovery Plan is essential. The DRP provides step by step procedures and processes required to ensure that services are returned to normal operation in the shortest possible time. The production and maintenance of such plans are the responsibility of the various IT staff assigned to any aspect of the network and IT services.

18. Breaches / Infringements

Failure to abide by these terms will be treated as misconduct.

Minor Infringements

For a first-time offence of a minor infringement, a warning will be issued. A second time offence will result in disciplinary procedures.

Serious Infringements

A serious infringement includes, but is not limited to, a third and subsequent offence of a minor infringement and will result in

- Referral to the appropriate disciplinary procedures; and/or
- Referral to law enforcement agencies (where the infringement constitutes a legal offence).

19. Responsibility

The EO is responsible for the review and implementation of this policy and the maintenance of all associated documents. Students, staff and relevant volunteers are required to sign and follow the BCAL IT user agreements appended below.

20. Legislative Context

Privacy and Data Protection Act 2014
Authorised Version 033 – 1 May 2026

Child Wellbeing and Safety Act 2005
Authorised Version incorporating amendments as at 23 February 2026
Authorised Version No. 046

Understanding Victoria's child safety laws