Contents

[Information Management 3](#_Toc81053766)

[Digital File Management 4](#_Toc81053767)

[Tracking Files 6](#_Toc81053768)

[Computer Standard Operating Environment (SOE) 8](#_Toc81053769)

[Computer Network Protocol and Viruses 9](#_Toc81053770)

[Archiving Files 11](#_Toc81053771)

[Computer Use 14](#_Toc81053772)

[Internet Use 15](#_Toc81053773)

[Email Use 16](#_Toc81053774)

[General Administration 18](#_Toc81053775)

[Communication Protocols 19](#_Toc81053776)

[Workplace Health and Safety - General 21](#_Toc81053777)

[Workplace Health and Safety – Ergonomics 25](#_Toc81053778)

[Workplace Health and Safety -Emergencies 30](#_Toc81053779)

[*Evacuation* 31](#_Toc81053780)

[*Bomb threat* 32](#_Toc81053781)

[Computerised and Manual Ledger 34](#_Toc81053782)

[Error correction 35](#_Toc81053783)

[Mail 37](#_Toc81053784)

[Environmentally Sustainable Work Practices 41](#_Toc81053785)

[Telephone Calls 44](#_Toc81053786)

[Equipment Consumables 48](#_Toc81053787)

[Equipment Maintenance 49](#_Toc81053788)

[Contracts by Tender and Quotation 52](#_Toc81053789)

[Exceptions to the requirement to seek tenders or quotations 53](#_Toc81053790)

[Acceptance of tender or quotation 54](#_Toc81053791)

[Petty Cash 55](#_Toc81053792)

[Reimbursement of Organisational Expenses 58](#_Toc81053793)

[Privacy Statement 60](#_Toc81053794)

[Risk Management 65](#_Toc81053795)

[Travel 70](#_Toc81053796)

[Human Resources 73](#_Toc81053797)

[Staff Training 74](#_Toc81053798)

[Staff Performance Review 76](#_Toc81053799)

[Staff Discipline 78](#_Toc81053800)

[Code of Conduct 81](#_Toc81053801)

[Conflict of Interest 85](#_Toc81053802)

[Employee Feedback 87](#_Toc81053803)

[Equity, Anti-Discrimination and Workplace Harassment 88](#_Toc81053804)

[First Aid 91](#_Toc81053805)

[Our Clients and Customers 93](#_Toc81053806)

[Client Complaints and Grievances 94](#_Toc81053807)

# Information Management

## Digital File Management

**Policy** Computer files are to be named and saved in a manner which allows employees to easily access their own files and the files for their program area on the network. All work-related documents should not be saved in personal drives or folders.

**Definitions Archiving** is the process of moving files from the system hard drive to another medium (e.g. tape or CD) to maximise the efficiency of the network. These files are still available for access when needed.

 **Backing up** is the process of duplicating data in file copy or file backup format from the system hard drive on to another medium so that they are available in the event of network failure.

 A **folder** (or directory) is a container in computer storage where files or other folders are stored.

 When a folder is created within a folder, it may be called a **subfolder** of that folder.

 A **document** is an individual record such as letter, report or spreadsheet.

Procedure

Network folder structure

The computer network is structured as follows:

Each program area has a folder.

In each of the folders for a program area, create subfolders to match the activity groups for that program area. These can be matched to the paper-based files for the program area.

Create a subfolder for templates.

Naming files

Name files so that they are easily located and accessed by all organisation employees.

If a second version of a document needs to be saved, add V2 (version 2) to the file name*.* Keep two versions of a document only when necessary.

Include the file name and path (drive and folders) at the end of the document or in the document footer.

**Saving files**

Save files in the relevant program area folder.

Do not save work-related documents in personal drives/folders.

Save lengthy documents regularly (at least every ten [10] minutes) while typing to prevent loss of data in case of computer or power failure.

File security

If files contain confidential (i.e. sensitive) information, add a password to the file to prevent unauthorised access.

Keep a record of these passwords in the secure online password repository.

Backing up files

Critical computer files should be placed in the enterprise’s network which uses a third party provided cloud storage system. This area is automatically backed up every 24 hours.

Our enterprise no longer backs up to on site resources.

Note our system technicians undertake a full site back up of data at the end of each month and this media is taken off-site for physical storage.

Archiving files

Check files at the end of each three months and decide which files can be archived.

Move these files to the archive section of the online cloud repository.

## Tracking Files

**Policy** The tracking of downloaded or physical files are monitored carefully to ensure the location of files removed from the filing system is known at all times.

**Definitions** **Open access files** are those files available to all employees.

**Confidential files** are those files for which access is restricted to specific employees (e.g. Manager and Program Supervisors).

Procedure

Removing a file

When removing or downloading a copy of an open access files from the filing system, record the details in the software application ***File Movement Register*** found on the desktop of each workstation.

**Confidential files** are only accessible to those employees specified under the relevant file number and name in the digital application ***File Register****.* This is set as an automated permission in the file access protocol of the digital network.

To access a **confidential** file, ask the File Supervisor. If granted access, the File Supervisor will record the details in the application *File Movement Register*.

Return physical files to the filing system within three (3) working days; digital files are to be copied to their location with changes within three (3) working days. If a digital file is nt changed, it must be deleted from the workstation after three (3) working day period. If a file is required for longer than three (3) working days, advise the File Supervisor when removing the file or before it is due for return.

Passing on a file

If a physical file is passed to another employee without returning it to the filing system, update the *File* *Movement Register.* It needs updating to show who has the file.

Returning a file

Return physical files to their relevant position in the filing system.

Record the date of return against the original record in the *File Movement Register*.

Overdue files

At the beginning of each week, the File Supervisor will identify overdue files from the *File* *Movement Register*.

The File Supervisor will notify all employees with overdue files and ask them to return the files.

## Computer Standard Operating Environment (SOE)

Policy The Standard Operating Environment (SOE) is to be specified by the General Manager to ensure security and consistency throughout the organisation.

Definitions SOE includes the specialised Operating System (OS) installed on the computer (i.e. Windows OS or Apple MacintoshOS applications and utilities), and other generic software programs.

Procedure

SOE structure

A suite of software applications common to all centres or work sites within our organisation (e.g. Microsoft Office, email – Microsoft Outlook, Internet browsers – Chrome, Edge and Firefox, virus protection software, our specialised software applications is to be installed on all computers and where appropriate digital devices.

Specialised software applications are restricted to:

* Point of Sale (POS) system
* Financial Administration System
* Customer Management System.

Installing additional applications

* If additional software is required to perform work activities, discuss its possible purchase and installation with the Team Leader and if acceptable, a business case can be made to the Director responsible for our IT infrastructure.
* No software applications are to be installed on workplace computers without the Director’s approval.

## Computer Network Protocol and Viruses

**Policy** Computer networks are used to enable the efficient and effective sharing of files.

**Definitions** A **login** is a code assigned to each organisation employee and recognised by the computer network. It authorises the holder of the code to access the computer network by keying in their password.

 A **password** is a code known only to an individual employee and is used to access the computer network.

Procedure

Access to the network

All employees should have access to the network so that files can be shared.

Login

Supervisors will specify a user login for each of their employees.

All login queries and problems should be referred to the Supervisor.

Password

Eachemployee must have a unique password of no more than eight (8) characters.

The password will be valid for 90 days after which it needs to be changed for security purposes.

No other person should have knowledge of an employee’s password.

All password queries and problems should be referred to the Supervisor.

Logging in to the network

Turn on the computer and screen.

When the login screen appears, type the password. (The last login will automatically appear in the login screen.)

All queries and problems should be referred to your Team Leader.

Exiting the network

Close all software applications according to the manufacturer’s instructions so that damage to, and loss of data is minimised.

Do not leave computers on overnight.

Viruses

All our organisation’s computers or digital devices come with pre-installed anti-virus software programs.

All computers are set to automatically check for viruses when they are turned on.

Take care when opening email attachments to ensure that email viruses are not introduced to the organisation.

Use of external digital storage media such as DVD-ROMs, flash drives and external hard drives should be scanned for viruses prior to opening. The anti-virus software is accessed from the appropriate icon found on all workstations’ desktops.

If a virus is detected, you will be prompted to follow directions, e.g. close files immediately or turn off the computer. If this happens, notify the IT Supervisor a nd your Team Leader immediately

The IT Supervisor will issue directions concerning specific viruses and all employees must follow these directions.

The IT Supervisor will contact the contracted computer technician for further advice.

## Archiving Files

**Policy** Archiving of files complies with legislative requirements *(Public Records Act 2002)* and ensures that critical information is not destroyed.

**Definitions Active records** are those records in frequent use regardless of their date of creation. They are needed for current business relating to the administration of the Organisation. These records are normally maintained in office space and equipment for easy access.

**Archiving** is the process of transferring or moving inactive information, including records from an active system to a repository for longer-term storage, preservation and access.

**Inactive records** are those records not in current use. They may be transferred to intermediate storage, archival custody or destroyed in accordance with an approved retention and disposal schedule.

 **Permanent** **records** are records which cannot be destroyed and must be retained indefinitely, either by the organisation or by Queensland State Archives.

 **Open access files** are available to all employees.

 **Confidential files** have restricted access to specific employees.

 For a full list of recordkeeping terms and definitions, see the *Glossary of Archival and Recordkeeping Terms* available on the Queensland State Archives website ([http://www.archives.qld.gov.au](http://www.archives.qld.gov.au/)).

Procedure

The Queensland State Archives administers the legislation for storing, transferring and disposing of public records.

To review current legislation (*Public Records Act 2002*), seek advice or further information about storage and disposal of public records refer to the *General Retention and Disposal Schedule for Administrative Records* located on the Queensland State Archives website at <http://www.archives.qld.gov.au/Government/disposal.asp>.

This *General Retention and Disposal Schedule for Administrative Records* provides guidelines for storing, transferring and disposing public records and covers areas such as:

* Annual report
* Bank accounts
* Celebrations
* Complaints
* Policies
* Publications
* Reporting
* Staff development
* Workplace health and safety

|  |
| --- |
| **Examples from General Retention and Disposal Schedule** **Queensland State Archives** |
| **Type of record** | **Status** | **Disposal action**  |
| Records relating to the development of Strategic Plans | Temporary | Retain for three years after last action |
| Records relating to the development of Operational Plans | Temporary | Retain for three years after last action |
| Records relating to mail including registers, certified and hand-delivered mail, messages etc | Temporary | Retain for two years after last action |
| Records relating to loan, lease or hire of equipment to other agencies | Temporary | Retain for one years after return of equipment or in the case equipment not returned, 5 years after last action |
| General Ledgers or Cash Books | Temporary | Retain for 20 years from end of last financial year  |
| Records relating to audits that lead to major changes in policies, systems or procedures of the organisation | Permanent | Retain Permanently |

Inactive records

* Go through the organisation’s files and separate those records that are inactive as suggested in the *General Retention and Disposal Schedule for Administrative Records*.
* Every inactive file should be reviewed individually and given a disposal action from the *General Retention and Disposal Schedule for Administrative Records*. This action should be recorded on the file and in the ***Records Storage and Disposal Register***.
* Put a date closed on each inactive file and record this date in the *Records Storage and* *Disposal Register*.
* Transfer open access records which are inactive to inactive storage. Pack the files into numbered boxes and clearly label each box with the contents and date range of the records. Store the boxes in a clean, secure area.
* Transfer confidential records which are inactive to the two bottom drawers in the *Confidential* filing cabinet.
* Record the transfer of all records in the*Records Storage and Disposal Register*.
* When the retention period specified by Queensland State Archives in an approved Retention and Disposal Schedule has passed, the General Manager will authorise the destruction of open access records. Confidential records must be shredded.
* Record the destruction of all records in the *Records Storage and Disposal Register*.

Permanent records

Retain permanent records for an indefinite period in the organisation.

## Computer Use

**Policy** All employees are required to comply with these procedures involving their use of BRTG computers.

**Definitions** Nil

Procedure

Opening and closing computers

Employees are to follow user procedures in switching on, logging on and shutting down their assigned desktop or laptop computer.

**Switching On the Desktop Computer**

The following steps must be observed in the computer starting procedure:

* Check that the power cables are connected to the surge protected general power outlets (green in colour).
* Locate and switch on the power buttons on the computer and where desktop units are in use, their screens/monitors.

**Logging On the Desktop Computer**

To log onto the computer, the employee must:

* Wait for the logon screen to appear.
* Enter the username and password for their computer.

**Switching Off the Desktop Computer**

The following steps must be observed when the employee is shutting down the computer:

* Check that any changes made in files have been saved and there are no open applications.
* Locate the power icon on the Start Menu and select shut down.

## Internet Use

**Policy** The Internet is accessible to staff for information for organisational purposes only.

**Definitions** Nil

Procedure

Access to the Internet

Employees should have access to the Internet for email and research purposes only if it supports their work role.

Time spent on the Internet

Internet time should be minimised to keep costs as low as possible.

Close the web browser application when not in use.

Personal use of the Internet

No personal research on the Internet is allowed without prior authorisation.

Any employee who accesses pornographic material through the Internet may have their employment terminated immediately.

These issues are covered by the *Code of Conduct*.

Downloading files

Downloading illegal files is strictly prohibited. These include any files without permissions for intellectual property rights, such as music, images and software/applications.

## Email Use

**Policy** Email is provided in all Bunjappy work sites for the purposes of the business. All employees must only use this service for work purposes and must do so in a professional manner that reflects positively on our enterprise. All employees are expected to follow these procedures.

**Definitions** Nil

Procedure

These procedures should be read and implemented in conjunction with the Email Style Guide.

Security

BRTG remains focussed on ensuring its digital data remains secure. Employees must only use secure digital platforms that provide encryption or other layers of protection for workplace information.

Email applications must have the security settings set to provide appropriate security for both incoming and outgoing correspondence.

Assignment

Each employee will be provided with a personalised email based on the first initial of the first name and the first four letters of their last name with a randomly generated three digit ending followed by the enterprise’s domain name.

Example: Jordan Francis jfran389@bunjappy.com.au

Some positions in the enterprise will have generic functional names for use, e.g. burdekin@bunjappy.com.au

Email structure

All enterprise emails must follow the outline and structure provided in the Email Style Guide.

Emails with attachments will only be limited to files that are relevant to Bunjappy’s business.

Attachments must not exceed the 20 Mb in file size limit.

Email with attachments must always include a brief description of the file/s attached in the body of the email.

All employees must confirm they received emails by responding to the email, unless it is a general workplace email notice, which does not require a response.

Issues or concerns brought up over email are considered official documentation and may serve as evidence if needed when resolving the issue.

Emails need to be stored in appropriate files. Refer to archiving policies and procedures.

Unimportant emails (which include spam and broadcast emails) may be permanently deleted on a daily basis.

Purpose of use

All employees will only use the provided Bunjappy account when sending official digital communications to fellow employees, clients, and other internal and external stakeholders.

Personal use

There is to be no personal use of the Bunjappy email service.

# General Administration

## Communication Protocols

**Policy** Communication systems enable the exchange of effective and efficient information.

**Definitions**  **External communication** is an exchange of information which occurs between the organisation and external parties, such as community members.

 **Internal communication** is an exchange of information which occurs within the organisation.

Procedure

General

Every organisation has its own cultural communication protocols. The information provided below reflects our workplaces and environment.

Methods of communication

**Internal communication**

* Use the following communication methods:
	+ **email** (whenever possible to save time and to provide a written record which is dated)
	+ **telephone calls** (between individual employees, to discuss and negotiate. Confirm with an email if necessary)
	+ **memorandums** (formally communicate information to other employees)
	+ **meetings** (to inform and discuss issues and make decisions. Note that meetings can be time-consuming and should only be held when communication by telephone, email and memorandums cannot achieve the desired outcome)

**External communication**

* Use the following communication methods:
	+ **emails** (where time is an important issue)
	+ **telephone calls** (to discuss or negotiate. Confirm any decisions by email, fax or letter.)
	+ **fax** (where time is an important issue and email is not an option either because it is not available or the information is in an unsuitable form for email)
	+ **letters** (to formally communicate information when time is not an issue.)

Responding to communications

Generally, respond using the same method as the original communication (e.g. if you receive an email, reply by email).

#### Timeframes

* Respond in the following timeframes wherever possible:
	+ Email same day
	+ Memos within three (3) working days of receipt
	+ Fax same day
	+ Letters within three (3) working days of receipt

Communication formats

* + Use the Style Guide for specific presentation guidelines.
	+ The following general guidelines apply:
	+ Use courtesy titles (Mr, Ms, etc) in the inside address of external correspondence. Use the addressee’s first name if the person is well-known to you.
	+ Do not use courtesy titles in the close of external correspondence.
	+ Do not use courtesy titles in internal correspondence (memos and emails).
	+ Letters should close with *Yours sincerely* if the addressee’s name is shown in the inside address; *Yours faithfully* if the addressee’s name is not shown in the inside address.

Inclusive language

* + Comply with cultural protocols by using correct titles, e.g. Aunty, Uncle, Misses.
	+ Use non-sexist and non-racist language by:
	+ avoiding male-dominated terms. For example, use ‘chair’ or ‘chairperson’ instead of ‘chairman’.
	+ eliminating the unnecessary use of the person’s gender, e.g. ‘female manager’
	+ avoiding the use of pronouns such as ‘he’ or ‘she’. Use ‘their’ instead of ‘his’ or ‘her’.

Signatures

The Manager of each of our centres is responsible for all organisation correspondence. These Managers may authorise other delegated persons to sign standard letters in some circumstances.

## Workplace Health and Safety - General

**Policy** The organisation aims to provide a workplace that is safe and free of risk to its employees’ health and welfare.

**Definitions** A **breach of workplace health and safety** is any activity, behaviour, equipment or furniture that does **not** comply with current workplace health and safety legislation and codes of practice.

A **hazard** is a dangerous or potentially dangerous situation that could result in a workplace illness, injury or death.

 A **hazardous substance** is one which must be used and handled with precautions and is likely to have a detrimental effect on a person’s health. The supplier may have to provide a Material Safety Data Sheet (MSDS) depending on the type of hazardous substance.

Procedure

Workplace health and safety philosophy

* The organisation takes its duty to provide all employees and community members with a safe and healthy working environment seriously.
* Workplace health and safety practices and processes are continuously reviewed to ensure that they comply with all relevant State workplace health and safety legislation.
* Workplace health and safety guidelines are designed to prevent accidents, injuries and illnesses in the workplace.
* All new employees must be made aware of workplace health and safety regulations and procedures during their induction program.

Management of Workplace Health and Safety

All issues and queries relevant to workplace health and safety should be referred to the respective Manager or team Leader.

Management must:

* Conduct regular audits of all equipment to ensure that they are properly maintained and serviced.
* Undertake an environmental risk assessment at least annually using the *Workplace* *Safety* *Checklist*.
* Report hazards or unsafe work practices to the WHS Manager.
* Assist Queensland Workplace Health and Safety inspectors.
* Investigate breaches of workplace health and safety and remedy the situation where possible.
* Investigate workplace incidents/accidents.
* Organise workplace health and safety training for employees.
* Promote health and safety in the workplace.
* Discuss workplace health and safety issues and provide information and advice to the relevant Manager or Team Leader.
* Review workplace incidents and make recommendations.

**Compliance**

Employees must:

* Follow all workplace health and safety legislation, regulations and guidelines including emergency procedures and drills.
* Immediately report any breach in workplace health and safety and any resulting injury or illness to the relevant Manager or Team Leader.
* Complete a ***Work Injury/Incident Report*** within 24 hours of the injury or incident.
	+ The Department of Industrial Relations requires notification of a serious incident within 24 hours.
* A serious incident defined by the Department of Industrial Relations includes:
* workplace incident involving a fatality.
* serious electrical incident involving a fatality.
* incident involving serious bodily injury or work-caused illness or dangerous event.
* serious electrical incident involving a shock or injury from electricity or dangerous electrical event.

 If uncertain, management should contact the Department of Industrial Relations to clarify.

* Identify potentially unsafe equipment, unsafe work practices, risks or hazards and ensure that other employees are aware of any potential danger/s. Make area safe in the short term.
* Complete the ***Employee Feedback Form*** to advise management of risks or hazards.

Department managers/supervisors:

* Ensure workplace is safe for employees.
* Check that employees are following workplace health and safety legislation, regulations and guidelines.

Reporting injuries/incidents

Employees who are injured or involved in a workplace incident:

* Notify the relevant Manager or Team Leader as soon as possible or ask a co-worker to notify the relevant Manager or Team Leader.
* Complete a *Work Injury/Incident Report* with the relevant Manager or Team Leader as soon as possible.
* The relevant Manager or Team Leader should complete this form if the employee cannot do it within 24 hours.

Relevant Manager or Team Leader:

* Complete the *Work Injury/Incident Report* if the employee cannot do it within 24 hours.
* Investigate the injury/incident to identify what can be done to prevent the incident happening again.
* Record any required preventative action on Part D of the *Work Injury/Incident Report*.

Hazardous substances

* When hazardous substances are received by the organisation, the details should be forwarded to the relevant Manager or Team Leader.
* A risk assessment must be completed to identify any hazardous substances.
* These hazardous substances should be added to the Register of Hazardous Substances by the relevant Manager or Team Leader.
* All hazardous substances are provided with a *Material Safety Data Sheet*.
* Training should be provided to employees who are exposed to hazardous substances.
* The Register of Hazardous Substances must be referred to when there is an incident involving hazardous substances.

Spills and leaks

Employees:

* Remove **spills** as soon as possible to minimise incidents.
* If a hazardous substance is involved, contact the relevant Manager or Team Leader to identify the method for removing the spill safely.
* Remove the spill according to instructions.
* Complete a *Work Injury/Incident Form*.
* If possible, repair **leaks** immediately.
* Complete a *Work Injury/Incident Form*.
* If it is not possible to fix the leak, notify the relevant Manager or Team Leader.

Manual handling

All new employees who are expected to lift or carry loads should receive training by an accredited trainer before commencing their duties.

* Keep the load as close as possible to the body.
* Avoid lifting:
	+ with the back fully bent
	+ with a twist or sideways bend to place the load
	+ for long periods with your back bent.
* Use mechanical handling aids (e.g. forklifts or trolleys) wherever possible.
* Modify the handling task to make it easier if mechanical aids are not available.
* Ask another employee for help.

All work processes that require regular manual handling should be risk assessed to minimise the risk of injury to employees.

## Workplace Health and Safety – Ergonomics

**Policy** The organisation aims to protect its employees’ health and welfare by providing furniture and a work environment which meets ergonomic requirements.

**Definitions Environmental factors** are those related to the work environment, such as noise and lighting.

 **Ergonomics** is the applied science of designing workplace equipment which is comfortable, safe and efficient to use.

Procedure

Workplace health and safety compliance

* The ***Workplace Health and Safety Policy and Procedure*** contains information on compliance.
* All issues and queries relevant to ergonomic and general workplace health and safety issues should be referred to the officer responsible for workplace health and safety within the organisation. This person is generally the relevant Manager or Team Leader.
* The relevant Manager or Team Leader will organise an assessment of all computers, furniture and equipment at least once a year to ensure that each employee’s work space meets both workplace health and safety regulations and ergonomic requirements.

Importance of ergonomics

Ergonomics applies to:

* posture
* prevention of fatigue and injury
* comfort and safety
* environmental factors, such as lighting and noise
* job, workstation and equipment design.

Ergonomically-sound work practices and equipment will help employees to:

* be more efficient.
* reduce or eliminate work-related injury.
* increase job satisfaction.

**Work environment**

**Glare and reflection**

* Shut or angle vertical blinds to block light and/or reduce glare if necessary.
* Do not position screens directly towards windows or fluorescent lights. Ideally, computer screens should be positioned at right angles to the windows and parallel to overhead fluorescent lights with a maximum tilt of 5º upwards.
* Use anti-glare filters (mesh covers, non-reflective glass).

**Noise**

* Equipment must not produce noise which exceeds the maximum noise level recommended by the Standards Association of Australia or as specified in local laws.
* If noise causes discomfort, report the problem to the Manager or Supervisor using the ***Employee Feedback*** form.

**Temperature**

* Report conditions which are too hot or too cold to the Manager and Supervisor using the *Employee Feedback* form.

**Radiation**

* While electromagnetic radiation is emitted from all electrical equipment, the extremely low levels are not considered to be a health risk.

**Workstation**

* Arrange all components of a work area to maximise good posture and minimise fatigue.

###

**Placement of items**

* Place items used regularly, such as the telephone, computer and calculator within easy reach.

**Chairs**

* Adjust to suit own requirements.
* When seated, adjust:
	+ back rest – the small of the back should be supported
	+ height of chair – feet should be flat on floor or on a footrest.

**Desks**

* Ensure feet are flat on the floor (or on a footrest) and knees or thighs are not in contact with the top of the desk.
* Arms should drop down vertically from the shoulders with forearms parallel with the floor when hands are in typing position.

**Keyboard**

* Position the keyboard so that the body’s midsection is slightly to the right of the centre of the keyboard.
* The keyboard should be 6-7 cm from the edge of the desk.

**Mouse**

* Place the mouse at either end of the keyboard depending on which hand is used to operate it.

**Computer screens**

* Computer screens should be:
* below the height of the individual’s eye, should be looking down onto the screen
* 60-70 cm in front of user.

**Footrests**

* Use a footrest if legs do not reach the floor when the chair, desk and keyboard are adjusted correctly. This will avoid pressure on the underside of thighs and support legs and feet.

**Document holder**

* The screen and document holder should be the same distance from user’s eyes.
* Ideally, the document holder should be attached to the computer screen, placed at an angle slightly to the left of the screen or placed between the screen and the keyboard to minimise eye movement.

**Posture**

* Hold body and head erect.
* Use a back rest to support the small of the back.
* Relax upper arms; tuck elbows slightly into the side, bent at approximately a 90° angle.
* Hold forearms and wrists horizontal or inclined slightly downwards.
* Make sure legs are clear of the front edge of the chair – no pressure on the underside of thighs.
* Feet are flat on the floor or on a footrest.

Ergonomic activities

**Eye breaks**

* Blink at regular intervals to help avoid eye irritation or dry eyes.
* Stop, stare into space or look out of the window at regular intervals to change the distance of vision.

**Work breaks**

* Take short breaks of 30-60 seconds while typing.
* After long sessions of typing, take a break and if possible, get up and move around.
* Do not remain seated for long periods.
* Vary tasks to avoid long sessions of typing.
* If pain or discomfort is felt:
* check posture.
* take a break.
* do some exercises.
* If pain continues, complete a *Work Injury/Incident Report* and discuss with the relevant Manager or Team Leader.

Exercise breaks

These exercises can be performed at any time throughout the day.

**Neck and shoulders**

1. Lower your head and then return it to an upright position. Then tilt your head back and return it to its original position. Do not do neck circles as they can injure your neck.
2. With your head upright, bend your head towards your left shoulder and then return.
3. Repeat, bending your head towards your right shoulder and then return.

**Hands and arms**

1. Place your forearms on a table and turn your palms up and down.
2. Hold your fingers out straight and spread first your forefingers, then your middle fingers and then bring them together again. Repeat this with all your fingers.
3. Touch each finger to your thumb and then repeat sliding the tip of your finger down to the base of your thumb.
4. With your fingers straight, bend your wrists to a 90° angle.

**Stretching**

1. Clasp your hands together and hold them out in front of your body.
2. Keeping your hands clasped, hold them above your head.
3. Then stretch to the right and to the left.
4. Place the palms of your hands on your chair and stretch your forearms.
5. Place your hands behind your head and stretch forward, backward and side to side.
6. Place your hands on your hips and hold your shoulders back.
7. Place your left hand behind your back at waist level and your right hand behind your back over your shoulder. Clasp your hands and stretch.

## Workplace Health and Safety - Emergencies

**Policy** The organisation aims to protect its employees’ health and welfare by ensuring that they are all aware of the way in which emergencies are handled.

**Procedure**

Management

* All issues and queries relevant to workplace health and safety should be referred to the Manager or Supervisor.
* It is a workplace health and safety requirement that all workplaces have an evacuation plan detailing exits and assembly points.
* All staff must ensure they are aware of the organisation’s evacuation plan.

Serious injury

* Do not panic.
* Do not move injured persons unless they are in a life-threatening situation.
* Make sure injured persons are in no further danger and make them comfortable.
* Send for first aid. Phone **000** if the injury is life-threatening.
* When phoning for help, tell the operator:
	+ where the emergency is
	+ what has happened
	+ what is being done
	+ who is calling.
* Do not hang up before being told what to do.
* Keep injured persons calm and warm if possible.
* Ensure airway is clear (apply resuscitation if required).
* After injury is dealt with, complete a ***Work Injury/Incident Report***.

Emergency phone numbers

**Life-threatening emergencies** 000

Poisons Information Centre 13 1126

Local hospital XXXX XXXX

Security (after hours) XXXX XXXX

 First Aid Officer Ext XXXX

### Evacuation

When the evacuation alarm sounds:

* + Do not panic.
	+ Collect personal belongings.
	+ Evacuate the area.
	+ Proceed to the assembly point via the nearest emergency exit. **Emergency exits** are via the stairs or fire escape. **Assembly points** are on the footpath directly opposite the relevant emergency exit.
	+ Move quickly but do not run.
	+ Use stairs. (If your building has lifts, do not use.)
	+ Assist disabled employees and visitors.
	+ Do not re-enter the building *under any* circumstance to retrieve personal belongings.
	+ If an accident occurs and someone is attending to the situation, do *not* stop; keep moving.

Team Leader:

* + Check work areas are evacuated and that employees have moved in an orderly way to the assembly point.
	+ Once employees are at the assembly point, account for all employees from the work area.
	+ Ensure employees and visitors remain at the assembly point until instructed otherwise.

##### Fire emergency

Employees should know be aware of the standards for fire safety:

* + smoke alarm signals and locations
	+ how to use fire extinguishers and fire blankets, etc
	+ where emergency exits are located
	+ where fire extinguishers and other fire equipment are located in their work area
	+ the purpose of each type of fire extinguisher
	+ how to operate the extinguisher/equipment.

In the event of fire:

* + Evacuate the immediate area of the fire: do not use lifts.
	+ Fight the fire only if it is safe to do so with the appropriate type of extinguisher for the fire.
	+ Ask another employee to telephone **000** with the fire details.
	+ Break the glass of the wall-mounted fire alarm and press the button.
	+ Contact the supervisor, if appropriate, and advise of the situation.
	+ Get down on hands and knees, if in a smoke-filled area, and crawl out. Cover nose and mouth if possible.
	+ Ensure all staff and visitors are accounted for.

### *Bomb threat*

**Threat by telephone**

* + Keep talking to the caller for as long as possible.
	+ Attract the attention of another employee. Ask them to notify the Manager or Supervisor before beginning a full evacuation.
	+ Try to find out where the bomb is located.
	+ **Do not hang up the phone.** If the caller does not hang up, the call may be traced.
	+ Take note of background noises, accents, or anything that may identify the caller.
	+ Cooperate with the police to provide as much information as possible about the caller.

**Suspicious article/package**

* + Do not touch or handle the package.
	+ Do not operate electrical devices in the area, e.g. mobile phones.
	+ Contact the Manager or Supervisor, giving full details of the suspect package.
	+ Follow the evacuation procedure.

Reporting injuries/incidents

Employees who are injured or involved in a workplace incident:

* + Notify the Manager or Supervisor as soon as possible or ask another employee to notify the Manager or Supervisor.
	+ Complete a *Work Injury/Incident Report* with the Manager or Supervisor within 24 hours if possible:

Relevant Manager or Team Leader:

* + If the employee is unable to complete the *Work Injury/Incident Report* within 24 hours, complete the form on the employee’s behalf.
	+ Investigate the injury/incident to identify what can be done to prevent the incident happening again.
	+ Record any required preventative action on Part D of the *Work Injury/Incident Report*.

**Debriefing**

If an emergency shall occur, it is recommended that all individuals undertake a debriefing session with management to re-assess the risks and the strategies to manage them.

A debriefing session may also be required with external qualified counsellors to enable staff and persons associated in the emergency to deal with the impact of the event on their working and personal lives.

## Computerised and Manual Ledger

**Policy** Ledger accounts are maintained accurately and updated regularly in a timely manner in compliance with ATO requirements and GST legislation.

**Definitions** An **audit trail** contains clearly defined document and ledger account references to enable a transaction to be traced through the accounting records.

 A **Chart of Accounts** is a list of all ledger account titles and their relevant account numbers.

 A **General Ledger** is a list of all account balances in the organisation.

 **Payable Reports** are listings of balances from supplier cards.

 A **Trial Balance** is a list of General Ledger account balances and is used to check the accuracy of the General Ledger.

**Procedure**

**Compliance**

All records must be maintained within the guidelines of the Australian Taxation Office, GST legislation, taxation legislation and *Australian Accounting and Auditing Standards*.

All accounts must be kept within the organisation’s computerised application, Financial Administration System.

**Chart of Accounts**

Ensure that all ledger entries are allocated to accounts in the standard Chart of Accounts.

If a new ledger account is required, identify the following information and discuss it with the Accountant:

* name of account, e.g. Motor Vehicles
* classification or group of accounts, e.g. Non-current Assets
* account number reference
* reason for creating new account.

A new ledger account must not be created without the Accountant’s authorisation.

**Source documents**

All documents must be checked and initialled prior to data entry. If possible, the person checking the documents should not enter the data.

**Journal/Cashbook entry**

The following documents are to be used as a source of data for entry into ledger accounts:

* cheques issued, direct debits (e.g. payroll deductions) and cash deposited either manually by an employee or through a direct deposit from outside the organisation
* miscellaneous source documents for General Journal transactions, e.g. accounts payable or accrued expenses at the end of the financial year where expenses have been incurred by the organisation but a payment has not yet been made

As a document is entered in the relevant journal, the document must be ticked and the date of entry recorded on the document. All document numbers must be entered accurately in the accounting records to ensure there is an audit trail. All journal entries must be checked against and reconciled with the batch of relevant documents

The following journals/books are to be completed as relevant:

* Cash book (to record receipts and payments)
* General Journal (to record adjustments)
* General Ledger (to record summary totals from cash book and adjustments from general journal)

**Posting to Ledgers**

Journal entries must be posted to the General Ledger, either at the end of the month or at the end of the financial year.

**Trial Balance**

At the end of each accounting period, a *Trial Balance* must be printed within three working days to check the accuracy of data entry in the General Ledger. Any errors must be identified and corrected before the *Trial Balance* is presented to the Accountant.

### Error correction

**Errors identified prior to processing of reports**

If an error is found in the current period’s accounts, the error is generally adjusted by correcting the entry for that transaction.

**Errors identified after processing of reports**

If an error is found after processing the financial reports and presenting the data, or in transactions from previous periods, the error is generally adjusted as follows:

* Cash book – Correct through reversing the incorrect entry and then re-entering the data.
* General Ledger – Correct through reversing the incorrect entry through the General Journal and then re-entering the data.

Refer errors to the Accountant where you are doubtful about how the adjustment should be made.

## Mail

**Policy** Mail is dealt with in a manner that promotes the efficient and confidential handling of all incoming and outgoing mail.

**Definitions Bulk mail** is a large quantity of outgoing mail which meets the specifications of Australia Post for bulk mail.

**Outgoing mail** is all correspondence and packages sent by the Organisation.

**Incoming mail** is all correspondence, facsimiles (faxes), magazines, circulars, advertising material and packages received.

Procedure

Managing mail

The assigned Administration Officer is responsible for managing and recording all incoming and outgoing mail.

Incoming mail

Collecting mail

The assigned Administration Officer will arrange to collect the mail from the local Post Office box assigned to a centre.

When mail is collected, it must be placed in a bag to ensure it is not lost.

Sorting incoming mail

Administration Officer:

Sort the incoming mail as soon as possible after it arrives.

Sort the mail into bundles:

* + mail marked ‘Urgent’ or sent by express post
	+ mail marked ‘Confidential’or ‘Personal’
	+ routine organisation mail
	+ parcels
	+ magazines, circulars and advertising material.

Before other mail is sorted, give priority to **urgent mail** over routine mail by:

* + date stamping it
	+ recording it in the ***Incoming*** ***Mail Register***
	+ distributing it to the relevant employee as soon as possible after receiving it.

Record **faxes** in the *Incoming Mail Register* and distribute them as soon as possible after receiving them.

Do not open **confidential** mail. If you open confidential mail in error, reseal it and attach a note, stating it was ‘Opened in error’, as well as the date and your signature.

Do not record confidential mail in the *Incoming Mail Register*.

Sort **routine organisation mail** by identifying the most relevant employee to handle the matter by looking at (in order):

* + name of the employee in the inside address or attention line
	+ title of the employee in the inside address
	+ program area in the inside address
	+ subject heading
	+ body of the letter.

Stamping incoming mail

Stamp all mail with the current date and time in an appropriate position (usually opposite the inside address on letters).

Checking incoming mail

Check incoming mail for:

* + return address
	+ damage
	+ contents and enclosures
	+ suspicious appearance or sounds.

Action required for missing return address

Check the envelope for a return address.

Staple the envelope to the letter if it contains the return address.

If you cannot find the return address, make a note on the letter; initial and date the note.

Action required for damaged mail

Contact the sender to verify that all items are in the package.

If items are missing, follow the procedure for missing contents.

Action required for mail with missing contents

If relevant, organise for replacement items to be sent.

If required, complete and submit insurance forms for damaged or missing items.

Action required for suspicious mail

Suspicious mail should not be handled.

Notify the Centre Manager immediately.

Recording incoming mail

Record **urgent mail and faxes** in the *Incoming Mail Register* as soon as they are received and then deliver them to the relevant employee.

Record routine business mail, parcels, magazines, circulars and advertising material in the *Incoming Mail Register* after urgent mail has been delivered.

Outgoing Mail

Checking outgoing mail

Ensure all outgoing mail has:

* + all enclosures attached
	+ been signed
	+ an address, including postcode
	+ matching letter and envelope, being sent to the same person.

**Delivery options for outgoing mail**

Depending on the geographic location of the organisation and the mail services available, outgoing mail may be sent by:

* + **standard mail** for routine items requiring standard delivery time
	+ **registered post** for items which require proof of posting and/or proof of delivery
	+ **overnight/express delivery** for those items requiring urgent delivery
	+ courier delivery for specialist delivery services especially for larger packages
	+ **bulk mail** for multiple items which meet the specifications of Australia Post for bulk mail.

Choose the delivery option taking into consideration the following factors:

* + cost
	+ time considerations
	+ delivery point location
	+ nature of the contents of the package (bulky, fragile, confidential)
	+ requirements for proof of posting and/or delivery
	+ quantity of items to be delivered.

In all cases, clarify and follow the requirements of the carrier, e.g. Australia Post.

Recording outgoing mail

Record all items and the amount of postage in the ***Outgoing Mail* *Register***.

Distributing incoming mail

* After all recording procedures have been completed:
	+ deliver **urgent mail and faxes** to the relevant employee or management committee member as soon as they are received
	+ deliver **magazines, circulars and advertising material** to the relevant work area for distribution (attach a *Circulation List* with names of those who should see the document if more than one)
	+ deliver all other mail and parcels to the relevant work area
	+ distribute relevant mail to the Management Committee, as appropriate.

## Environmentally Sustainable Work Practices

**Policy** Bunjappy recognises the importance of protecting the environment and will minimise the environmental impact of work practices carried out by the organisation.

**Definitions Environmentally sustainable work practices** are those which reduce harm on the environment and reduce wastage of resources.

Procedure

General guidelines for sustainable environmental work practices

All employees can help protect the environment by following the guidelines below:

**Reduce**

* Use goods which stop waste being generated.
* Reduce waste by choosing products that have minimal packaging and can be used productively and then recycled.

**Re-use**

* Re-use containers, packaging or waste products, wherever possible.

**Recycle**

* Recycle waste material into useable products, wherever possible.

**For waste that can't be avoided, reused or recycled**

* Treat the waste to make it less harmful or reduce the volume of the harmful component.
* Dispose of the waste safely.

Strategies to be implemented by the Manager and Supervisors

* Consider sustainability issues when making planning and managing decisions.
* Promote and encourage environmental awareness to ensure employees are aware of their environmental responsibilities.
* Aim to continually improve environmental performance by identifying and addressing environmental risk.
* Make resources available to implement environmental risk management procedures.

Employees’ responsibilities

* Identify and manage environmental risks associated with work activities to minimise their impact on the environment.
* Use the ***Employee Feedback Form***to put forward suggestions.

Managing safety risks

Employees

* Be aware of workplace health and safety policies and ensure procedures are followed.
* Notify the Workplace Health and Safety Officer of specific risks or hazards by completing an *Employee Feedback Form*.

A safety risk assessment must be undertaken by the Workplace Health and Safety Officer at least once a year using the ***Workplace Safety Checklist***.

Environmental purchasing guidelines

* Become informed about the environmental impacts of products purchased. Search for environmentally-friendly products.
* Choose products with less packaging.
* Choose products with recyclable or reusable packaging.
* Re-use plastic bags and all types of containers if possible.
* Buy quality goods that will last.
* Buy recycled goods which have already saved resources and raw materials and help reduce the overall quantity of waste.

Paper wastage

* Buy and use recycled paper where possible.
* Make double-sided copies when printing and photocopying, wherever possible.
* Use the blank side of used paper for notepaper before recycling.
* Re-use envelopes for internal mail.

Disposal of waste

* Place the following in recycle bins, depending on recycling facilities available in your community.
	+ paper
	+ aluminium
	+ glass
	+ steel
* Follow the guidelines for the disposal of these materials to minimise the impact on the environment.

Energy

* Use these strategies to minimise energy wastage:
	+ Maintain air-conditioning at a constant temperature of 23-24ºC.
	+ Close blinds or curtains to minimise heat build-up.
	+ Maintain only security lighting after business hours.
	+ Switch off equipment overnight wherever possible.
	+ Repair malfunctioning utilities (e.g. leaking taps) as soon as possible.

## Telephone Calls

**Policy** All telephone calls are handled in a professional, courteous and prompt manner.

**Definitions Standard telephone phrases** are the responses which should be used by employees of the organisation to deal with specific telephone situations.

Procedure

Incoming calls

Answering the call

Answer all incoming telephone calls by the third ring.

Calls to the general telephone number will be answered by the Administration Officer and transferred to the relevant extension as necessary.

Standard telephone phrases to be used

The following phrases should be used when answering incoming telephone calls:

|  |  |  |
| --- | --- | --- |
| **Incoming call situation** | **Reception** | **Program area** |
| External call  | *Good morning/afternoon (name of organisation). May I help you?* | *Good morning/afternoon, . . . . speaking.* |
| Internal call  | *(Name) speaking.* | *(Name) speaking.* |
| Transferring calls to extension | (Repeat the name of the person wanted.) *One moment please.*If the extension is busy:*That extension is busy now. Would you like to hold or may I take a message?*If the person is unavailable:*(Name) is not available now. May I take a message?* |  |
| Taking a telephone message | Take the message and repeat the details back to the caller.  | *Take the message and repeat the details back to the caller.*  |

|  |  |  |
| --- | --- | --- |
| Incoming call situation | Receptionist/Administration Officer | Other employee |
| Screening a call (If the Manager or other employee asks for their calls to be screened.) | When caller asks for Manager/ employee:*May I ask who’s calling please?*When speaking to Manager/ employee to see if they will take the call:*(Name) wishes to speak with you. Do you wish to take the call?*When the Manager/employee wishes to take the call:*. . . I am transferring you now.*When the Manager/employee does not wish to take the call:*. . . is unavailable now. May I take a message?* |  |
| Ending a call | *Thank you for calling. Goodbye.*Let the caller hang up first. | *Thank you for calling. Goodbye.*Let the caller hang up first. |

Telephone messages

Record the message on a ***Telephone Message Slip***.

Include*:*

* + Name and organisation
	+ phone number
	+ message
	+ date
	+ time

Repeat the message back to the caller to ensure the details you have recorded are correct.

After the call, place the *Telephone Message Slip* in the employee’s in-tray as soon as possible or email the message.

Creating messages on answering machines or a voicemail service

Follow the manufacturer’s or telephone company’s instructions when creating a message.

The message should be: (Name) is not available now. If you leave your name and number, (name) will get back to you as soon as possible.

For organisations that are only open on certain days or for limited periods of time, the message could be: Hello, you’ve reached Bunjappy’s Regional Tourism office at (specific location stated) our office hours are between (e.g. 7.30 am to 5.30 pm, Monday to Friday). If you leave your name, a contact number and a brief message, someone will call you back as soon as possible.

Personal telephone calls

Keep personal calls to a minimum. While all employees will receive personal incoming calls, the quantity and length of these calls needs to be monitored so they do not affect the employee’s capacity to undertake their assigned duties.

**Outgoing calls**

Preparing for the call

* + Check the telephone number before dialling.
	+ Make notes of points to raise with the other person.

Placing the call

Dial 0 and listen for dial tone.

Then dial the number.

Standard telephone phrase to be used

Use the following phrase when making outgoing telephone calls:

*Good morning/afternoon. This is . . . from . . .(state which Bunjappy cantre).*

STD, ISD and mobile numbers

Limit the length of these calls to minimise telephone charges.

If possible, phone during times when economy rates apply.

Personal telephone calls

Keep personal calls to a minimum and within the local area – no overseas or interstate calls.

## Equipment Consumables

**Policy** Equipment is operated so that repairs, maintenance and the use of consumables are minimised.

**Definitions Business equipment** includes photocopiers, facsimile machines, printers and binders.

A **consumable** is a resource required to maintain the equipment or to complete a task using equipment, e.g. toner and paper.

Procedure

Paper

Consult the manufacturer’s manual to identify the most appropriate weights and types of paper which can be safely used in business equipment (e.g. photocopiers and printers).

Place the paper in the equipment according to the manufacturer’s instructions.

Keep a minimum of three (3) reams and a maximum of ten (10) reams of A4 paper in a cupboard close to the equipment. The amount of paper and other consumables that needs to be stored depends on the availability of supply. If supplies are not readily available because the organisations is located in a remote community, then more consumables need to be kept in stock than if suppliers are located nearby.

Store remaining paper in a secure location.

Toner

When the toner is empty, remove the toner cartridge from the equipment item and place it in the original box.

When a replacement cartridge is needed, present the empty cartridge in its box to the Administration Officer, as a reminder that a new cartridge needs to be ordered.

Used cartridges are to be recycled where the facility is available or otherwise disposed of appropriately.

Store the empty box in a cupboard close to the business equipment.

**Other consumables** (including staples, plastic covers and binding combs)

Consult the manufacturer’s manual to identify the appropriate type and size of consumable required.

Store a small quantity of each consumable in a cupboard close to the equipment.

Store all remaining supplies in a secure location.

Notify the Administration Officer when additional quantities are required.

## Equipment Maintenance

**Policy** Equipment is operated in accordance with manufacturer’s instructions and in a way which minimises the cost of repairs and maintenance.

**Definitions Business equipment** includes photocopiers, facsimile machines, printers, binders and other specialised machinery.

Procedure

Management of maintenance

The Administration Officer manages the maintenance of all equipment under the supervision of the Manager.

Operation of equipment

Operate all equipment in accordance with the manufacturer’s instructions and workplace health and safety procedures.

Faults

When an equipment fault is detected, read the manufacturer’s manual to identify the type of fault and the steps required to fix it.

Do not try to fix any fault where the manual specifies that the manufacturer must be contacted. This may void the warranty or the service agreement.

For **minor faults**, follow the manufacturer’s instructions closely to minimise further damage to the equipment.

* + If you cannot fix a minor fault, follow the procedure for major faults.

For major faults, complete an *Equipment Fault Report.*

* + Submit the *Equipment Fault Report* to the Administration Officer who will notify the relevant equipment supplier.
	+ The Administration Officer will place an ‘Out of Order’ sign on the equipment item, showing when the fault will be rectified.

The Administration Officer retains all *Equipment Fault Reports* as a record of an item’s reliability.

**Maintenance**

Consult the manufacturer’s instructions to identify the maintenance required for each item of equipment. The Administration Officer will ensure that the recommended maintenance schedule is followed.

The Administration Officer will organise both minor and major maintenance of equipment.

**Safety checks**

A qualified electrician should check all electrical equipment annually.

The Administration Officer is responsible for organising the safety checks.

A test tag should be attached to the power cord of each item of business equipment to indicate that it has passed the annual check.

The Administration Officer must be told of any items not carrying the test tag.

## Contracts by Tender and Quotation

**Policy** The organisation is comitted to open and transparent processes in the selection of approved contracts and tenders.

**Definitions** **Contract** – an agreement by law between two parties

 **Tender** – an offer made in writing by a party to carry out certain work or supply goods

**Procedure**

The organisation will ensure:

* All suppliers will be required to have an Australian Business Number (ABN).
* Procurement of goods and services is carried out in a way that is open, transparent accountable and serves and protects the community’s interest.
* Ethical behaviour and fair dealing in the selection of approved contracts and tenders i.e. not a conflict of interest or bias.
* Contract or tenders are financially sound, i.e. there is value for money.
* Contracts and tenders will enhance the organisation’s service delivery.

**Prior to entering into a contract**

Any contract made, varied or discharged by the organisation must be signed by the authorised signatories, under the common seal.

The responsible officer should ensure that:

* The contract amount is within the approved budget figure for the purchase in the current financial year.
* Procedures for authorising have been followed.
* Approval has been obtained.

**When tenders are required**

Before making a contract for the supply of goods or services, or the carrying out of work involving a cost of more than $100,000 (or a designated amount that is prescribed by the constitution or organisational policy), the organisation will invite tenders through:

 (a) placing an advertisement in the local newspapers

 (b) placing an advertisement in other newspapers if the scope of work to be carried out or goods and services required cannot be obtained from within the local area, and

 (c) allowing at least 21 days from the day of the advertisement for the submission of tenders.

**When quotations are required**

Before making a contract for the supply of goods and services or carrying out of work involving a cost less than $100,000, or amount otherwise prescribed by legislation, the constitution or organisational policy, the organisation’s purchasing officer must invite written quotations from at least 3 suppliers who can meet the requirements of the organisation at competitive prices.

### Exceptions to the requirement to seek tenders or quotations

The organisation may choose to make a contract under an exemption to open tender in the following circumstances:

 (a) under a standing offer or a preferred supplier arrangement

 (b) with a supplier from a register of pre-qualified suppliers

 (c) it resolves that it is satisfied that there is only one supplier reasonably available to it

 (e) it resolves that a genuine emergency exists

 (f) it resolves that it is satisfied that the services to be supplied are of such a specialised nature that it would be impractical or disadvantageous to the organisation to invite tenders or quotations

 (f) it resolves to obtain second-hand goods

 (g) it resolves to purchase goods at an auction.

**Register of preferred or pre-qualified suppliers**

The organisation may decide to prepare a register of suppliers suitably qualified to provide a service by:

(a) inviting expressions of interest from suppliers through an advertisement process.

(b) following the stated procedures in this policy as the basis when selecting persons to provide the service.

**Changes to tenders**

The organisation can may make changes to tenders if:

(a) tenders were invited for the contract and

(b) the invitation to tender states that the organisation might later invite all tenderers to change their tenders.

The organisation may invite all the persons who have submitted a tender to change their tender to take account of a change in the tender specifications before a decision is made on the tenders.

### Acceptance of tender or quotation

The organisation will accept a tender or quotation most advantageous to it.

The organisation will have regard to the objectives of this policy when deciding on which tender or quotation is the most advantageous.

 The organisation may, however, decide not to accept any tender or quotation available to it.

## Petty Cash

**Policy** Petty cash is used to make cash payments to reimburse/pay back employees who have paid for expenses on behalf of the organisation.

**Definitions** The **petty cash fund** is the amount established to pay for petty cash expenses. The amount in the petty cash fund should be enough to cover petty cash expenses for a minimum two-week period. This amount is often $50 or $100. The Petty Cashier controls this fund.

 A ***Petty Cash Voucher*** is a form completed by an employee who wants to be reimbursed for an organisation-related expense or who wants an advance to pay for such an expense.

A **petty cash advance** is an amount issued from petty cash to allow an employee to pay for an organisation-related expense.

 The ***Petty Cash Book*** is used to record all *Petty Cash Vouchers* and is balanced fortnightly, or as necessary.

 The **petty cash box** is a locked container which contains the cash for the petty cash fund.

 The **Petty Cashier** is the employee who is responsible for maintaining the petty cash fund and petty cash records. This person is usually the Administration Officer.

 The **Authorised Officer** is the person in the organisation who is given the job of checking that documentation is correct before payment is made. This person could be someone from the Management Committee or the Manager but is not the bookkeeper.

**Procedure**

Petty cash fund

The Manager should regularly review the amount in the fund to ensure that the amount is adequate.

The money should be kept in a locked petty cash box under the control of the Petty Cashier.

Petty cash expenses

Petty cash expenses must be related to legitimate organisational activities.

The maximum limit for petty cash expenses is $100. Expenses over this amount must be paid by cheque.

Casual wages arenot paid out of the petty cash fund.

Documentation required

Employees:

Keep all dockets and/or receipts for petty cash expenses as proof of payment.

Attach dockets and/or receipts to the back of the ***Petty Cash Voucher***.

Record the amount of the expense plus GST on the *Petty Cash Voucher*.

Check at the point of purchase that dockets/receipts are clear and correct.

Claims process

Employees:

Complete a *Petty Cash Voucher*(GST value should be shown on the *Petty Cash* *Voucher*).

Attach relevant dockets/receipts to the back of the *Petty Cash Voucher.*

Obtain the supervisor’s authorisation for amounts over $50.

Submit all claims to the Petty Cashier within seven (7) working days.

Petty Cashier:

Check the claim and reimburse the employee from the petty cash fund for the amount spent within two (2) days of the claim.

Petty cash advances

Employees:

Complete a *Petty* *Cash* *Voucher* if money is needed, in advance, to pay an organisation-related expense.

Get the Manager’s approval for the advance.

Give the Petty Cashier a docket/receipt for the money spent, as well as any change from the advance, within five (5) working days of receiving the money.

Security

Petty Cashier:

Keep the petty cash fund secure by:

* + not allowing other persons access to the petty cash box
	+ locking the petty cash box when it is not being used
	+ putting the petty cash box in a locked desk drawer during working hours
	+ putting the petty cash box in a safe place overnight.

Do not issue funds from the petty cash fund unless a *Petty Cash Voucher* has been processed, in accordance with the above guidelines.

Petty cash expenses

Petty Cashier:

Check all *Petty Cash Vouchers* against dockets/receipts for accuracy.

Check that all claims are related to the organisation’s business.

Check that all claims over $50 have been authorised by the employee’s supervisor.

Pay approved petty cash claims promptly and accurately.

Keep all *Petty Cash Vouchers* in the petty cash box until recorded.

Petty cash advances

Petty Cashier:

Check that all petty cash advances are authorised.

Pay out petty cash advances.

Follow up petty cash advances if the docket/receipt for the expense is not submitted within five (5) working days.

Petty Cash Book

Petty Cashier:

Record all *Petty Cash Vouchers* in the ***Petty Cash Book*** at least weekly.

Balance the *Petty Cash Book* fortnightly or when funds are running low.

Check the balance in the *Petty Cash Book* against the amount remaining in the petty cash box.

Submit the *Petty Cash Book* and *Petty Cash Vouchers* to the Authorised Officer fortnightly and advise of any problems.

Advise the Authorised Officer of how much money is required to reimburse the fund (bring it back to its original amount).

Advise the Authorised Officer when the amount in the petty cash fund needs to be increased.

## Reimbursement of Organisational Expenses

**Policy** The organisation will reimburse authorised organisational expenses evidenced by supporting documentation.

**Definition** Authorised officer refers to the employee/management committee member who has been delegated the authority to approve payment.

**Procedure**

**Types of organisational expenses**

It is preferable to pay for organisational expenses by purchase order and cheque. However, in some cases, petty cash or cheques may be used to reimburse expenses incurred.

The following items are examples of expenses that may require reimbursement.

|  |  |
| --- | --- |
| **Item** | **Organisation related expenses** |
| Catering  | To provide refreshments for meetings with official visitors, e.g. cake, tea/coffee  |
| Taxi  | To cover costs of taxi fare to attend meeting, conference, workshop, etc. |
| Petrol/Mileage Allowance | To cover cost of petrol to attend meeting (if petrol cards not available) |
| Stationery | To cover costs of purchasing essential or urgent stationery items |
| Telephone | To cover costs of work-related telephone calls from home or mobile phone (approval required) |

**Reimbursement process**

Prior to approving reimbursement, the Manager or relevant authorised officer:

* must be satisfied that any claim for reimbursement has been for official purposes
* must sight supporting documentation (supplier’s invoice and evidence of payment) that clearly states
	+ date and amount of expenditure
	+ name of company/service provider
	+ description of the expense incurred.

Employees cannot authorise payment or reimbursement to themselves. If the Manager or authorised officer needs to be reimbursed, it should be approved by the Chairperson or Treasurer of the Management Committee.

When the authorised officer is satisfied that the expenses were for official purposes and the required documentation has been received, the employee should be reimbursed as soon as possible.

The original receipt and documentation are to be retained for the organisation’s financial records.

## Privacy Statement

**Policy** This organisationis committed to protectingthe privacy of our employees and clients. We will comply with its obligations under the *Privacy Act 1998*.

Definition This policy declares the intentions of our organisation in relation to client and employee information and data, how personal information is stored, how clients and employees can access this information and the purposes for which personal information is used and disclosed.

Focus The policy objective includes:

* the right to privacy, dignity, and confidentiality is recognised and respected;
* data privacy and protection in adherence to the principles stipulated in the Australian Privacy Principles (APPs) and the Information Privacy Principles and the Health Privacy Principles (HPPs);
* methods for managing personal information are open and transparent;
* information obtained for relevant purposes only; and,
* regulation of access and correction of personal information may occur.

The policy applies to all persons within and involved in Bunjappy Regional Tourism Group and its affiliates.

Procedure

**General Principles**

* All information relating to employees and customers is treated confidentially.
* Personal information will not be released to another person without consent, except in the instances where our organisation is legally obliged to do so.
* Employees have the right to access their own records in the presence of a Manager after making a written application to do. Access to their personal files would occur within 21 days of the receipt of the written request.

**Personal Information**

BRTG collects and holds the personal information of employees, volunteers,

Contractors and customers. The personal information held may include some of the following:

Employees

Name

Date of Birth / Country of Birth

Address and contact details

Details of Next of Kin

Occupation

Employment history

Employment Application Form

Citizenship, Passport, and Visa permit

Medical history or fitness for work information

Employment References

Tax File Number

Bank Account Details

HR/Personnel records including Superannuation Fund

Workers’ compensation or injury information

Qualifications, training, and competency records.

**Volunteers**

Name

Date of Birth / Country of Birth

Address and contact details

Details of Next of Kin

Occupation

Volunteer Application Form

Qualifications, training, and competency records.

**Contractors**

Name

Address and contact details

Qualifications, licenses, etc.

Contractor Agreement

Insurances including Workers Compensation, Professional and Public Liability

**Customers/Clients**

Name

Current address and contact details

Relevant Medical information dependent upon activity selected

Financial and Billing information (i.e. credit card details)

**Data collection**

Bunjappy collects personal information to ensure it can provide both our clients and employees with the most appropriate assistance. The information is collected in a fair, legal and transparent way.

Consistent with the company’s obligations under Australian law, such as but not limited to tax office obligations, and industrial instruments, this enterprise only collects personal information considered necessary for the fulfilment of these legal requirements as well as the provision of services as outlined in the enterprise’s objectives.

In general, such personal information will be obtained directly from the individual provided consent from the individual is given.

Collecting personal information can be done through the following methods:

* forms or telephone calls
* written information sent through letters, faxes and e-mails
* face to face meetings
* bookings

In cases where the personal information is collected from sources other than those mentioned directly from the persons concerned, Bunjappy will inform the persons concerned. Unsolicited information considered unnecessary and irrelevant to operations of the enterprise will be removed from our records.

When people access our website, there is no attempt to identify the person as an individual user, and personal information is not collected unless the user specifically provides this to our company, e.g. through an online form. Information recorded and logged by our website’s Internet Service Provider may include the address, top-level name (e.g., .com, .gov, .org, .au, etc.), date and time of entry, type of web browser, information accessed such as pages and documents. Our website management group may use statistical data collected by our ISP to evaluate the effectiveness of our website. BRTG are required to allow law enforcement agencies and relevant government agencies with the proper authority to inspect our ISP logs, if an investigation warrants such an inspection. Our website uses temporary ‘cookies’ to identify and interact more effectively with a user’s computer. A ‘cookie’ is a small text file placed on the website’s visitor’s computer by the webserver when they access our website. Our use of temporary cookies means that when a visitor closes their browser, no personal information is retained that may identify that visitor.

**Data storage**

Information collected by BRTG while a person is accessing our services is kept in a personal file. Files are stored in a secure, digital locations within a cloud-based repository.

For further information on data storage, please see the policy document, Digital File Management.

**Data use**

BRTG will only use the personal information collected for the purposes for which it was collected, or other purposes that are agreed to between this enterprise and the client. Additional purposes may be required to comply with legislation. If this is the case, BRTG will communicate to the client that this has occurred.

**Disclosure of Personal Information**

Personal information will generally only be disclosed by authorised persons.

Personal information may be disclosed if Bunjappy:

* Are required by Australian law or obligated through a court/tribunal order.
* Reasonably believe that the disclosure of such information is necessary to lessen or prevent an imminent threat to an individual’s life, health or safety, or a significant threat to public health or safety.
* Have reason to believe that any unlawful activity has been, is being, or can be engaged in.

If it is necessary to transfer personal information interstate or overseas, as per the provisions of Privacy Act, the proper steps will be followed to make sure that the Act will not be violated in relation to said information.

Personal information relating to persons will not be used for other purposes such as fundraising or direct marketing activities without seeking written consent.

**Security of Personal Information**

BRTG will take appropriate action to protect personal information against misuse and loss and against unauthorised access, alteration or disclosure.

All personal information will be viewed as confidential and all reasonable steps to ensure that personal information is secure will be taken.

To comply with legal responsibilities, all Bunjappy’s digital data systems that hold personal information have current security protection systems and are subject to regular review to ensure these are effective, efficient and able to meet any potential interference that might occur.

All employees with access to the personal information of clients and other staff are trained in the accountabilities and obligations of their positions.

Records are disposed of in a safe and responsible safely.

If BRTG does suffer the loss of personal information, the General Manager will:

* act to identify and secure the incident in order to prevent further incursions into our data systems;
* assess the seriousness and nature of the damage or loss;
* initiate an internal investigation as to how the incident occurred and who was responsible for the loss;
* report the breach to the Police where criminal activity is suspected;
* notify the Privacy Commissioner of cases concerning a significant breach of security and individual privacy; and,
* inform the individual(s) concerned where appropriate and possible.

**Access by an individual**

An individual can access their own personal information from the Bunjappy Regional Tourism Group. Our organisation undertakes to ensure this access is:

* convenient
* without reasonable delay
* without cost.

**Further information on privacy**

For further information, contact The Office of Privacy Commissioner on the toll-free number 1300 363 992 or 1800 620 241 (for hearing impaired only, no voice calls).

You can also email the commission at privacy@privacy.gov.au or access the website address at [http://www.privacy.gov.au](http://www.privacy.gov.au/)

## Risk Management

**Policy** The organisation identifies and manages risks in a systematic and cost-effective manner.

**Definitions** A **risk** is the possibility or likelihood of something happening which may have a negative impact on the organisation’s capacity to deliver on its strategic and operational plans.

 **Risk management** is the process which is used to avoid, reduce or control risks.

Procedure

Types of risks

Examples of risks include:

* client dissatisfaction with service delivery
* harm caused to management committee, staff, volunteers, clients or the public
* loss of government funding
* equipment
* inadequate allocation of resources, e.g. human, physical and financial
* financial mismanagement
* fraud
* breaches of confidentiality
* service disruption or closure.

Why manage risks?

* Risk management is a fundamental part of sound organisational management.
* The organisation will not be able to eliminate all risks but they can take active steps to prevent or minimise the likelihood level and impact of risk by developing a **Risk Management Plan**.
* An annual risk management plan should be prepared and reviewed as part of the Strategic and Operational Planning Process.
* By managing risks, the organisation is better placed to:
	+ protect the safety and well-being of staff, volunteers, clients and visitors
	+ provide efficient and effective service delivery
	+ manage and maintain facilities and equipment
	+ improve confidence and public perception of the organisation
	+ operate within the allocated budgets
	+ protect or reduce likelihood of legal action
	+ comply with legislative or funding requirements.

Responsibilities for risk management

* All employees are responsible for identifying, reporting and managing risks.
* The General Manager must approve and sign off the Risk Management Plan.
* Managers and Team Leaders are accountable for implementing and maintaining sound risk management processes in their work areas. This includes creating a culture and environment in which employees are encouraged and supported to identify and manage risks.

Reporting

Team Leaders:

* Report regularly on assessment and management of risks in work area.
* Update the ***Risk Register*** for their work area every three months.

Manager:

* Review all risks identified and the measures proposed or undertaken to manage them.

General Manager:

* Monitor and evaluate the implementation of the Risk Management Plan.

Risk management process

**Step 1 Analyse the context**

* Consider the environment in which the organisation operates to establish the boundaries in which risks must be managed and guide decisions on managing risks.
* The financial, operational, competitive, political, public perception/image, social, cultural and legal aspects of the organisation’s functions are all part of the risk management context.

**Step 2 Identify the risks**

* Identify the risks (what can go wrong) that arise from all aspects of the environment outlined in Step 1. Include:
	+ community perception/image
	+ political (e.g. government funding)
	+ cultural
	+ physical and environmental
	+ financial
	+ legal
	+ ethical or moral.

**Step 3 Evaluate the risk**

**High risk**A high level of risk requires close monitoring and immediate action where needed as the potential loss or negative impact could be devastating to the organisation.

**Medium risk** A medium level risk requires normal levels of monitoring action where required, as the potential loss or negative impact could be significant.

**Minor risk**A low level of risk can be treated with routine policy and procedures as the potential loss or negative impact is likely to be small.

The table below summarises steps 2 and 3.

1. **Probability** - How likely or how often will this risk occur: rare, likely or very likely?
2. **Seriousness** - How serious would the consequences or the impact of the risk occurring, be on the organisation: minor, medium or major?
3. **Priority** - Based on the probability and the seriousness, what priority should your organisation give to managing the risk: low, medium, high? The priority assigned impacts on the action required.

|  |  |
| --- | --- |
| Probability | Seriousness of Consequences (impact) of Risk(Minor, Medium Major) |
|  | Minor | Medium | Major |
| Rare | Low | Low | Medium |
| **Likely** | Low | High | High |
| **Very Likely** | Medium | High | High |
|  | **Priority Rating**(Low, Medium or High) |

**Step 4 Manage the risk**

* The organisation will need to determine one of the following options to manage the risk:
	+ **Avoid the risk.** The organisation might decide on a different course of action rather than take the risk involved in the original course of action.
	+ **Transfer the risk.** The organisation might shift responsibility for the risk to another person or organisation (e.g. take out insurance against the risk).
	+ **Reduce the risk.** The organisation might reduce the likelihood or consequences of the risk by adopting a strategy such as regular training, progress reporting on major activities or auditing risk management procedures on a regular basis.
	+ **Accept the risk.** If all other options are not available to the organisation, they might decide to accept the risk but put in place policies and procedures to manage it.

The organisation then needs to develop a risk management plan. Ask:

* + What can be done about the risk?
	+ How can we prevent or reduce the likelihood of the risk occurring?

**Step 6 Monitor and review**

* Regularly monitor and evaluate the strategies used to manage risk.
* Risks do not remain the same. The environmental context changes and other factors have an impact.

Ways to reduce risks

* Develop and implement good strategic/operational planning, financial management and community engagement processes.
* Develop and monitor good risk reducing policy and procedures for staff, e.g. code of conduct, project planning, critical incident reporting.
* Develop a Risk Register.
* Plan for unseen events.
* Make sure that security measures are in place.
* Develop and implement effective reporting processes.
* Check that all assets (e.g. equipment) are in safe working order.
* Develop and maintain sound financial management practices.
* Place signs, notices or instructions regarding possible risks, e.g. *Wet Floor*
* Make sure that facilities, utilities and equipment are maintained regularly.
* Make sure that staff receive adequate safety induction and training.
* Make sure that staff is effectively supervised.

## Travel

**Policy** All travel by employees must be undertaken in a manner which achieves the outcomes required and reduces expenses and time wastage.

**Definitions** The **traveller** is an employee who is travelling on behalf of the organisation.

Procedure

Approvals

All travel for employees of the organisation must be approved by the General Manager.

The assigned Administration Officer is responsible for notifying the General Manager of any expenses which need to be prepaid on behalf of the traveller.

Air fares

Fares booked must be refundable and booked as soon as possible after travel has been approved to take advantage of any discounts available.

Electronic check-in is to be used. The traveller is responsible for providing two forms of identification when checking in at the airport.

All travellers travel economy class.

Car hire

The organisation is billed directly for all car hire by the car hire company.

After the trip, the traveller should forward all car hire documents to the Administration Officer for checking before the account is paid.

Taxi fares

Travellers should pay for taxi fares. Submit receipts to the assigned Administration Officer for checking, recording and recoupment of funds expended.

Accommodation

Accommodation booked must be within the current allowance specified by the organisation.

Where possible, accommodation will be booked and paid in advance by the Administration Officer.

Other travel expenses

Travellers with the organisation’s credit cards should use these cards to pay for incidental travel expenses and meals.

* Travellers should forward all receipts to the Administration Officer after the trip for checking and recording.
* Travellers without an organisation credit card should use their own cash or credit card to pay for incidental travel expenses, unless directed otherwise by the Manager.
* These travellers will be reimbursed for these expenses after the travel is completed and on presentation of receipts.
* A ***Travel Expenses Claim***shouldbe completed. Attach all receipts to the form and submit the form to the Administration Officer.

Itinerary

Administration Officer:

Prepare an itinerary for the traveller showing:

* + dates of travel
	+ details of flights
	+ accommodation
	+ appointments.

Make four (4) copies of the itinerary for distribution as follows:

* + one on file for reference
	+ one for the employee who is acting in the traveller’s job role
	+ one for the Manager as relevant
	+ one for the traveller’s partner/family.

Travel folder

Administration Officer:

Prepare a travel folder for each Traveller including:

* + itinerary
	+ relevant documentation
	+ blank Travel Expenses Claim.

Submit the travel folder to the traveller at least four (4) days before travel.

Ask the traveller to check all travel details and clarify any issues.

# Human Resources

## Staff Training

**Policy** Employees receive opportunities to undertake training to improve their personal prospects for promotion and increase the organisation’s capacity.

**Definitions** Nil

Procedure

General

By providing training to its employees, the organisation increases its capacity to achieve long-term goals and to meet the ongoing needs of the community. Training can benefit both individual employees and the organisation by improving motivation, commitment and retention.

Supervisors and the Manager are responsible for identifying the skills required by employees to meet the goals outlined in the organisation’s Strategic Plan.

Identifying employees’ training needs

Employees must complete a ***Staff Training Needs Self-Assessment*** before their performance review interview.

The *Staff Training Needs Self-Assessment* will be discussed at the performance interview and the training required to improve the employee’s skills will be identified.

Program Supervisors may identify specific skills needed in their work areas. They will consider employees who would be most suited to training in these skill areas.

Employees may also identify training which they feel will help them do their work. The Manager may approve the training if the cost is within the Organisation’s training budget and will increase the skills available to the Organisation.

Applying for training

The Manager approves all training undertaken by Program Supervisors and employees.

Program Supervisors and employees must complete a ***Staff Training Application*** form with details of the training and submit it to the Manager for approval.

Training costs

The costs of training and the time taken out of the workforce to complete training will be dependent on the employees’ individual work contracts with the organisation.

Some employees may be eligible to undertake training during working hours, with no loss of pay and the organisation meeting the costs of the training.

Some employees may receive training outside normal working hours at the cost of the organisation or the employee.

Some employees may have to meet the costs of any training that an employee undertakes.

Evaluating training

After undertaking training provided or paid for by the Organisation, a Program Supervisor or employee must complete a ***Staff Training Evaluation*** form and submit it to the Manager within five (5) working days.

The evaluation will be used to assess the value of both internal and external training programs. It will also be used to discuss how learnings from the training can improve practices and be shared with other work colleagues.

## Staff Performance Review

**Policy** Employees of the organisation will undergo a performance review annually to assess performance, identify areas for improvement and specify any training needs.

**Definitions** Nil

Procedure

Organisation of performance review

Performance reviews are conducted by the Manager or the employee’s Program Supervisor every year or as required.

The Program Supervisor will organise appointments for performance reviews with their employees.

The Manager will conduct Program Supervisors’ performance reviews.

Preparation for performance review interview

The Manager or Program Supervisor will notify employees in writing, two weeks in advance, of the date and time of their performance review.

Employees should complete a ***Staff Training Needs Self-Assessment*** before the date of the review. They should take their self-assessments to the performance interview.

The Manager or Program Supervisor will review the performance of their employees over the past year and make notes for the interview.

Conduct of performance review interview

Annual performance reviews seek to:

* + clarify any issues relevant to the employee’s job description and performance standards
	+ identify the employee’s strengths
	+ identify areas where the employee needs to improve
	+ discuss the *Staff Training Needs Self-Assessment* completed by the employee and any training that will help the employee improve their skills
	+ make changes to the employee’s *Staff Training Needs Self-Assessment*, where necessary. (Both parties must sign this document as agreement on the employee’s training needs.)
	+ identify training/development activities that are required
	+ identify and confirm the actions to be taken to improve performance.

All employees will be interviewed by the Manager or their Program Supervisor. Either party can request that the Manager be present during the interview.

The ***Staff Performance Review Feedback*** will be completed by the Manager or Program Supervisor and signed by that person and the employee.

Where strategies for performance improvement are required, a ***Staff Performance Improvement Plan*** should be completed and signed by the employee and supervisor.

Training

After the Staff Performance Review, a ***Staff Training Plan*** should be completed and signed by both the employee and their supervisor.

One copy of the completed *Staff Training Plan* should be sent to the Manager for information purposes.

One copy of the completed *Staff Training Plan* should be filed in the employee’s file.

If internal or external training is to be undertaken, a ***Staff Training Application***should be completed at least five (5) working days before the date of training.

The relevant Manager or Team Supervisor is required to approve the *Staff Training Application*.

After training has been undertaken, a ***Staff Training Evaluation*** form must be completed within ten (10) days.

Discrimination

If employees believe that they have been directly or indirectly discriminated against in the performance review, they should contact the General Manager.

## Staff Discipline

**Policy** Employees who are not performing satisfactorily or engage in misconduct or do not comply with the organisation’s Code of Conduct may face disciplinary action.

**Definitions** Nil

Procedure

Guidelines for supervisors

* To minimise problems:
	+ conduct a formal induction program for new employees
	+ provide job descriptions so that employees are aware of their duties
	+ ensure new employees are aware of, and understand the *Code of Conduct*
	+ ensure employees are aware of this policy and procedure
	+ follow this policy and procedure when problems arise
	+ identify problems as soon as they arise and take action
	+ maintain records of all performance-related discussions and counselling sessions
	+ ensure that fairness to employees is balanced with the needs of the employers (organisation) to dismiss employees when there is a good reason.
* The employer should ensure that in all processes that the principles of natural justice are followed. This involves the employee having an opportunity to state their point of view before action is taken and that the decision maker must not be biased.
* High staff turnover should be avoided because of the costs involved and loss of productivity.

Misconduct

If an employee engages in serious misconduct that is unreasonable for the employer to continue the employment, the employee may be dismissed instantly. Examples of misconduct by an employee include theft, assault and fraud.

Any such action would need to be supported by a high level of evidence.

Other misconduct that may result in disciplinary action:

* non-compliance with the *Code of Conduct*
* breach of the behaviour guidelines in the *Code of Conduct*
* prevention of other employees from carrying out their duties.

If the above conduct or misconduct occurs, the employee’s Supervisor must complete a ***Misconduct or Non-Performance Report*** detailing relevant incidents and/or behaviours and submit it to the Manager.

The Supervisor should notify the employee that they intend to write the report.

The Supervisor should provide the employee with a copy of the completed *Misconduct or Non-Performance Report*.

Non-performance

If supervisors identify unsatisfactory performance of an employee, they will advise the employee on their performance problems.

Training may be required to improve the standard of the employee’s performance. An opportunity must be provided for the employee to improve their performance within a reasonable timeframe.

If the employee's performance does not improve to the required standard after assistance and training within the specified time, the Supervisor must complete a *Misconduct or Non-Performance Report* outlining specific performance problems.

The Supervisor should submit the *Misconduct or Non-Performance Report* to the Manager.

The Supervisor should provide the employee with a copy of the *Misconduct or Non-Performance Report*.

Discipline for misconduct/non-performance/Breach of Code of Conduct

After a *Misconduct or Non-Performance Report* is submitted to the Manager, the following disciplinary process must be followed:

Discussion/Counselling

The Manager will organise a disciplinary session with the employee and their Supervisor. The Manager will attend this session. The problem will be explained and the employee asked to respond. The employee is entitled to have a support person present.

If misconduct or non-performance/breach of Code of Conduct is proved, the Manager will advise the employee of the corrective action they need to take.

The Supervisor will record details of the disciplinary session in the *Misconduct or Non-Performance Report*. The Manager, Supervisor and the employee will sign the report.

First warning

If the incident of misconduct/breach of Code of Conduct is repeated or performance does not improve, the Supervisor will inform the Manager. The Manager will issue a first written warning.

If the case is considered severe enough, the first warning could be regarded as the final warning.

Final warning

If the problem persists, the Manager will issue a final written warning to the employee. If the problem is not resolved, the Manager will take action to dismiss the employee.

The Manager will maintain formal records (*Misconduct or Non-Performance Reports)* of each counselling/disciplinary session and keep them confidential. All records must be sighted and signed by the relevant employee as true. Such records will provide important evidence if the matter proceeds to the Queensland Industrial Relations Commission.

Dismissal

The organisation must comply with all State and Federal legislation and the employee’s terms/contract of employment in relation to administering discipline and the termination of employment. Please refer to the relevant contact detail of the Queensland Department of Industrial Relations in the Resources Section.

The organisation must ensure:

* dismissal is not for an unfair reason
* employee knows the reason for dismissal and has an opportunity to respond to the employer in relation to that reason
* they give the employee appropriate notice or compensation in lieu.

Putting the reason for dismissal in writing will help to clarify the situation and prevent any misunderstandings.

Employees may be dismissed on the basis of:

* + their conduct, capacity or performance
	+ operational requirements, e.g. the position is no longer required
	+ other reasons sufficient to justify termination.

**Resources**

The Queensland Industrial Relations Commission administers both the Industrial Relations Act 1999 (state legislation) and the [Workplace Relations Act 1996](http://www.airc.gov.au/procedures_and_legislation/wra_index/) (non-Queensland Government link).

[The Industrial Relations website](https://www.qirc.qld.gov.au/)

## Code of Conduct

**Policy** Employees and Management Committee members adhere to the organisation’s Code of Conduct which reflects the behaviour expected and is designed to encourage integrity and professionalism.

**Definitions** A **Code of Conduct** is a set of rules, regulations and guidelines which employees are expected to observe during their employment.

Procedure

Code of Conduct philosophy

The organisation prides itself on the professionalism and ability of its employees and Management Committee to meet community needs. The organisation strives to be a leading service provider and to provide a safe, healthy and happy workplace.

This Code of Conduct is designed to ensure that all employees, Management Committee and community members are treated in a manner that reflects the mission, culture and legal obligations of the organisation.

Compliance

* All employees and Management Committee members are expected to:
* observe all policies, procedures, rules and regulations at all times
* comply with all Federal, State and local laws and regulations
* comply with all reasonable, lawful instructions and decisions related to their work
* maintain a high degree of ethics, integrity, honesty and professionalism in dealing with community members and other employees
* adhere to the Workplace Health and Safety Policy and Procedure
* maintain the confidentiality of the organisation’s operations in relation to service activities, confidential documentation and work practices during and after their employment
* take reasonable steps to ensure their own health, safety and welfare in the workplace, as well as that of other employees and community members. Employees are expected to make themselves familiar with their workplace health and safety obligations.

Employee and Management Committee behaviour

* If an employee breaches the following guidelines, disciplinary action may be taken.
* If the breach of conduct is of a legal nature, it will be addressed in accordance with relevant Federal, State or local government laws.
* Employees and Management Committee members should not:
	+ discriminate against another employee or community member on the basis of sex, age, race, religion, disability, pregnancy, marital status or sexual preference
	+ engage in fighting or disorderly conduct, or sexually harass other employees and community members
	+ steal, damage or destroy property belonging to the organisation, its employees or community members
	+ work intoxicated or under the influence of controlled or illegal substances
	+ bring controlled or illegal substances to the workplace
	+ smoke on the organisation’s premises or in its motor vehicles

accept benefits or gifts which give rise to a real or apparent conflict of interest.

Dress code

* + - Employees and Management Committee members **should**:
* dress to comply with workplace health and safety regulations relevant to their work activities
* dress suitably for their position, presenting a clean, neat and tidy appearance at all times
* wear minimal jewellery
* wear a uniform (if supplied) and maintain its condition (clean and not torn)
* consult with the Manager or Program Supervisor if unsure of the type of clothing appropriate to their position.
	+ - Employees who deliberately breach this dress code may receive disciplinary action.

Privacy and confidentiality

Securely store personal information provided by a client or employee.

Take reasonable steps to ensure this material is kept secure against:

* + loss
	+ unauthorised access
	+ use
	+ modification or disclosure
	+ misuse.

Use personal information only for the purposes for which it was collected. Do not disclose personal information to another party unless the individual is aware of, or has consented to, the disclosure.

Keep information about all service provision confidential within the organisation. Do not disclose information associated either directly or indirectly, to the organisation to external parties unless authorised by the Manager or Program Supervisor.

Dealing with aggressive behaviour

Employees are expected to provide high standards of service provision but the organisation does not accept any form of aggressive, threatening or abusive behaviour towards its employees by community members.

If an employee is unable to calm the person and/or believes the situation places them or other employees in danger, they should notify the Manager or their Program Supervisor.

Use of computers, telephones, facsimiles

* + - Unauthorised access and use of confidential information can severely damage the reputation of the organisation and undermine personal privacy.
		- Employees and Management Committee members **should**:
* use communication and information devices for officially approved purposes only
* use these communication and information devices for limited personal use, as long this use does not interfere with their daily duties
* not share their password/s with another employee or share another employee’s password/s.

Use of the Internet and email

* Internet and email are provided to employees and Management Committee members for genuine work-related purposes.
* Employees and Management Committee members **should**:
* limit personal use to a minimum. The organisation may monitor use and call upon employees to explain their use.
* comply with copyright regulations when using the Internet or email.
* Employees and Management Committee members **should** **not**:
* divulge personal or confidential information via the Internet or email
* use the Internet to access websites or send emails of an explicit sexual nature or in any manner that breaches the *Equity, Anti-Discrimination and Workplace Harassment Policy and Procedure*.
* While the privacy of all employees is respected, emails may be used as evidence if legal action is taken against an employee.
* This information may also be used as evidence of a breach of the *Code* *of Conduct* or the *Equity, Anti-Discrimination and Workplace Harassment Policy and Procedure.*

## Conflict of Interest

**Policy** Employees, executive management members and other work leaders will declare potential, perceived and/or real conflicts of interests. The organisation will engage in open, transparent and ethical decision-making processes.

**Definitions Pecuniary interests** arealso known as financial or fiscal interests.

A **potential conflict of interest** occurs whenthere is a risk that the matter could be considered a conflict of interest.

A **real conflict of interest** occurs when there is an actual conflict of interest.

 **Disclosed conflict of interest** - an open declaration of a conflict of interest.

**Procedure**

* A **conflict of interest** occurs when an employee’s personal interests are in conflict with the organisation’s interest. When there is a conflict, it may influence the outcome of the decisions they are required to make.
* A **personal interest** occurs when a decision a person makes directly or indirectly affects themselves or associates including (but not limited to):
* immediate and extended family members or other persons with a strong personal bond (e.g. husband, wife, children, brothers, sisters, parents, cousins, aunts, uncles and friends)
* organisations in which the person is actively involved (church, sporting club, etc)
* business partner/s.
* A **personal or material interest** occurs when a person and/or their associates may indirectly or directly stand to profit from the decision personally or financially being made by the decision maker.
* If an employee of the organisation believes they have a potential or real conflict of interest in a matter that requires a decision to be made, the employee should disclose the personal interest to the General Manager. For example, if the organisation is deciding whether or not to fund an all-expenses-paid trip for a young employee to attend a conference and the person is a son or daughter of a executive management member or an employee, the employee must declare the conflict of interest.
* If an employee of the organisation believes they have a personal interest that may result in their financial gain, the employee must declare the interest to the General Manager.
* If the General Manager believes that a potential or real conflict of interest may exist, then then they are required to disclose the matter to the organisation.

**What happens when a conflict of interest is disclosed?**

* When an employee declares a potential or real conflict of interest at a meeting, the disclosure should be recorded in the Minutes. Other than that, the employee is required to disclose the potential or real conflict of interest through the submission of a memo or letter to the General Manager outlining the details of the issue.
* When a conflict of interest is disclosed, the General Manager should record the declaration in the *Conflict of Interest Record*.
* When the employee discloses a conflict of interest, the responsibility for resolving the conflict rests with the person to whom the disclosure is made.
* If the conflict of interest is a minor issue, the organisation may decide that disclosure and registering the conflict of interest is a sufficient course of action.
* If the conflict is significant, the organisation should implement a policy that the person who has the conflict must remove themselves from all discussions and decisions being made regarding the matter.

**Accessing the Conflict of Interest Record**

* The *Conflict of Interest Record* should be stored in a safe and secure location. The General Manager in consultation with the executive management team will decide who may access the *Conflict of Interest Record.*

##

## Employee Feedback

**Policy** Employees are encouraged to provide comments or suggestions to improve services, processes and procedures.

**Definitions** Nil

Procedure

Comments or suggestions for improvement

Supervisors/Team Leaders:

* + Encourage employees to put forward their comments or suggestions for service, process or procedural improvements by completing an ***Employee Feedback Form*.**
	+ Consider these comments or suggestions.
	+ If necessary, discuss them at the next team meeting.

Employees:

* + Complete an *Employee Feedback Form* to submit comments or suggestions for improved services, processes and procedures.

Workplace health and safety hazards

* + Employees should notify the Workplace Health and Safety Officer of workplace hazards by completing an *Employee Feedback Form*.
	+ If the hazard is serious, it will be removed or repaired as soon as possible.
	+ If the hazard is not serious, it will be discussed at the next staff meeting.

Personal issues

Employees:

* + Try to resolve issues of conflict with other parties before taking matters further.
	+ If the conflict cannot be resolved, discuss the matter with the Program Supervisor.
	+ If the conflict involves the supervisor and cannot be resolved, discuss the matter with the Manager.
	+ Advise the Program Supervisor of personal issues that may affect work performance.
	+ Discuss issues of sexual harassment or discrimination with the Program Supervisor or Manager.

## Equity, Anti-Discrimination and Workplace Harassment

**Policy** Bunjappy Regional Tourism Group is an equal opportunity employer and its employees are expected to conform to equity and anti-discrimination guidelines.

**Definitions Discrimination** occurs when someone is treated less favourably than another in similar circumstances because of a personal attribute that has no relevance to the situation.

 **Equity** allows all employees to be treated fairly and without discrimination.

**Sexual harassment** is any form of unwanted, unwelcome or uninvited sexual behaviour that is offensive, humiliating or embarrassing.

**Workplace harassment** is repeated behaviour, other than behaviour amounting to sexual harassment, of one employee or group of employees that is unwelcome, unsolicited, and considered to be offensive, intimidating, humiliating or threatening by another employee.

Procedure

Equity and anti-discrimination philosophy

* Our organisation strives to provide a positive working environment in which all employees are valued and encouraged to contribute.

Our organisation is bound by all relevant State and Federal legislation in relation to Equal Employment Opportunity (EEO). This legislation ensures that no employee will be discriminated against unfairly or unlawfully.

* Work practices and processes are continuously reviewed to ensure they comply with EEO requirements. These work practices include:
* recruitment and selection
* pay and benefits
* training and development
* promotion
* discrimination and harassment
* performance appraisals/reviews
* grievance procedures
* terminations.

Compliance

* Employees must neither be discriminated against nor discriminate, treat unfairly or unlawfully another employee or community member on the following grounds:
* sex
* race, colour, nationality or ethnic origin
* religion
* disability
* age
* pregnancy
* marital or parental status
* political belief or activity
* trade union activity
* lawful sexual activity
* association with or relation to a person with any of the above attributes.

Harassment

* Employees should not be subject to, or engage in unlawful harassment or discrimination against another employee or community member in a manner which is unwanted, intimidating or offensive.
* Forms of harassment include:
* sexual harassment
* homosexual and transgender vilification
* HIV/AIDS vilification
* racial vilification.
* Sexual harassment includes:
* unwanted attention or touching
* sexual propositions
* leering or staring
* offensive language
* displaying nude images
* persistent requests for dates
* crude or offensive jokes.
* Harassment will not be tolerated and disciplinary action will be taken against those responsible.

Inclusive language

* When writing internal or external documents, ensure that non-sexist and non-racist language is used by:
* avoiding male-dominated terms (e.g. use ‘chair’ or ‘chairperson’ instead of ‘chairman’)
* eliminating the unnecessary use of the person’s gender (e.g. ‘female Manager’)
* avoiding the use of ‘he’ or ‘she’ (use ‘their’ instead of ‘his’ or ‘her’).

Breaches of EEO

All breaches of EEO will be taken seriously.

Complaints will be dealt with promptly and in accordance with relevant State and Federal legislation.

All complaints will remain confidential.

Employees who feel that they are victims of discrimination or harassment:

* Approach the Manager to discuss appropriate actions or options.
* Lodge a formal complaint or grievance which will be dealt with by the Manager.

## First Aid

**What is it? First Aid** refers to the immediate response and treatment applied to a person involved in an accident. In extreme circumstances, the timeliness and quality of first aid given to a person could mean the difference between life and death.

 **The information contained in this document is to be used as an introductory guide only.**

**Administering First Aid**

The organisation should take active steps to ensure that they have first aid equipment, trained staff and the facilities to handle injuries or illnesses in the workplace.

* First aid is only to be administered by a qualified employee in the event of minor accidents or in situations where an injured person needs to be stabilised until an expert assistance arrives, e.g. ambulance officer or doctor.

The organisation should aim to have:

* First aid management plan that needs to be completed upon initial commencement of the organisation and reviewed at least yearly.
* minimum of one staff member (preferably two) with a current Senior First Aid qualification that incorporates Cardio-Pulmonary Resuscitation (CPR) qualifications.
* fully equipped first aid kit that will be in a safe and secure location
* fully equipped first aid kit located in vehicles if the service or organisation has designated vehicles for use by staff and clients.
* First Aid Officer to regularly check that the first aid kit is fully stocked, wherever possible
* readily available list of persons and services that provide medical assistance, e.g. OOO number, local hospital, doctors and community health centres, Poison Service
* compliance with relevant legislation and organisational policies specifically related to handling first aid matters, e.g. critical incidents and emergencies
* record of when first aid has been administered. This record should include:
	+ date first aid administered
	+ who received first aid
	+ reason for receiving first aid
	+ who administered first aid
	+ what treatment/response was provided
	+ any further action.

**First Aid Officer**

This employee should:

* be adequately qualified to administer basic first aid (Senior First Aid Certificate)
* be able to remain calm in an emergency
* be reliable and diligent in the maintenance of the first aid kit and facilities
* ensure all staff, volunteers, clients and visitors are notified of incidents that can impact on their health and safety.

**What is in a First Aid Kit?**

First Aid equipment is essential for an organisation to effectively manage injury or illnesses in the workplace.

A guide regarding first aid kits has been provided below. However, for more detailed information regarding first aid kits, please contact your local St Johns Ambulance service on telephone 1300 360 455 or access the [St John website](http://www.stjohn.org.au/).

For organisations exposed to low level of risks or accidents, the first aid kit should contain, but limited to, the items listed below:

* adhesive strips (band-aids) for minor wound dressings
* scissors
* safety pins to secure bandages or slings
* triangular bandages for slings
* gauze pads for cleaning wounds
* tweezers to remove foreign objects
* ice pack for the treating strains, sprains and bruises
* dressings to control bleeding and cover wounds
* antiseptic solutions for cleaning wounds and skin
* disposable gloves for infection control
* sterile saline solution
* small bowls for holding cleaning solutions
* non-allergenic adhesive tape for securing strapping and dressings
* eye pads for emergency eye cover
* plastic bags for waste disposal
* sharps disposal container
* note pad and pencil for recording injury, conditions and treatment given.

# Our Clients and Customers

## Client Complaints and Grievances

**Policy** The organisation is committed to handling and resolving client complaints in a confidential, fair and timely manner.

Definitions Nil

Procedure

Types of Complaints

There are many factors that influence a client’s decision to make a complaint. There is also a range in the types of complaints that can be made. Examples of factors and types of complaints include:

Service delivery complaints

* dissatisfaction with service provision
* accuracy and timeliness of information
* communication breakdown
* cultural issues
* stress and fatigue
* incidents of conflict
* inappropriate behaviour of staff and volunteers
* poor maintenance of facilities and equipment
* client abuse, harassment, discrimination and neglect
* breach in client confidentiality.

Governance complaints:

* financial mismanagement
* fraud
* procedures followed not in accordance with the organisation’s constitution or organisational policies.

Complaints of potentially criminal nature:

* If the complaint has criminal implications, such as fraud or abuse, then the Police should be notified immediately.

Methods of complaint

There are two ways clients may choose to make a complaint to the organisation:

* verbal – face to face or by phone
* written – formal letter, e-mail, fax.

Anonymous complaints

* Some clients may wish to remain anonymous in making their complaint. This should be respected and the complaint investigated.

Responding to complaints

* All client complaints should aim to handle and resolve every complaint immediately, wherever possible, using the following process:

Verbal complaints

* It is suggested that employees:
* listen carefully and respond to the client in a polite and respectful manner
* clarify your understanding of the complaint and ask the client how they would like the complaint resolved. Wherever possible, try to resolve the complaint at the time.
* If the circumstances do not allow the complaint to be resolved immediately, direct the complaint to the Manager.
* If the Manager is unavailable, the complaint should be directed to the staff member with the most appropriate skills to handle the matter, e.g. Workplace Health and Safety Officer (WHSO).
* If the client wishes only to speak with the Manager, arrange a meeting between the Manager and the client at a time that is mutually convenient.
* Advise the client that they may submit the complaint in writing. See *Client Complaint Form.*
* Follow the process for written complaints below.
* Record complaint in the *Client Complaint Log*. For guidance refer to the *Client Complaint Log (sample).*

Written complaints

* All complaints of a serious nature, e.g. corruption, fraud, harassment, etc. should be submitted in writing and referred to the Manager for investigation. If the complaint involves the Manager or the client feels that the Manager is not the appropriate person to handle the complaint, refer the matter to the Chair of the Management Committee.
* Upon receiving a written complaint, the Manager or Management Committee should aim to provide a response within ten (10) working days.
* The response may include the following:
* confirmation that the complaint has been received and the matter is being investigated
* an understanding of the complaint
* suggested actions for resolving the complaint
* complaint process, including the estimated timeframe for resolution
* client satisfaction and right to appeal
* contact name and number.

**Appeals and seeking outside assistance**

* If the complaint involves the General Manager, the matter can be referred to the Management Committee.
* If the complaint cannot be resolved internally, an option could be to seek support from the Dispute Resolution Branch of the Department of Justice and Attorney General.

Dispute Resolution Branch

Floor 1
Brisbane Magistrates Court
363 George Street
Brisbane Qld 4000

GPO Box 149
Brisbane Qld 4001

Ph: (07) 3239 6269
Toll free outside Brisbane 1800 017 288
Fax: (07) 3239 6284

* If the complaint still cannot be resolved, the client should be informed that they have the right to make a complaint to the Office of the Ombudsmen.

Queensland Ombudsmen

Level 25, 288 Edward Street
Brisbane QLD 4000
GPO Box 3314
Brisbane QLD 4001

Tel: 07 3005 7000
Toll Free (outside Brisbane): 1800 068 908
Fax: 07 3005 7067
TTY: 3006 8174
Email: ombudsman@ombudsman.qld.gov.au

Website: <https://www.ombudsman.qld.gov.au/>