Policy 3	INFORMATION MANAGEMENT SYSTEMS

Record of policy development		
Version	**Date approved**	**Date for review**
3.5	**December 2020**	**December 2022**
3.4	**May 2019**	**January 2021**
3.3	**June 2018**	**October 2020**

Policy purpose: Coastlink has effective information management systems in place

Policy:

COASTLINK information is a corporate asset, vital both for ongoing operations and also in providing valuable evidence of business decisions, activities and transactions.

There is an expectation that COASTLINK will meet, and strive to exceed, the expectations of funding bodies, key stakeholders and legislation, in its commitment to the handling of all information. COASTLINK is committed to creating and keeping accurate and reliable information to meet this obligation.

COASTLINK will implement fit-for-purpose information management practices and systems to ensure the creation, maintenance and protection of reliable information. All information management practices in COASTLINK are to be in accordance with this policy and its supporting procedures.

Principles:

There are four factors which ensure that management of an organisation is adequately informed:

1. An organisational performance framework: This sets the overall expectations for how the organisation will perform, and provides a systematic way for senior staff and the board or management committee to assess this on a regular basis.
2. A management information system (MIS): A MIS provides to managers and other senior staff a continuous flow of information about the activities within an organisation.
3. A reporting system: Reporting systems ensure that critical information about progress and issues requiring attention pass from staff to managers, and from managers to the board.
4. A research and development process: Development of an organisation's services and activities, and planning of its future directions, needs to be informed by a combination of external information on a range of relevant areas and internal

information about organisational performance.
Relevant Standards
NSW Disability Service Standards:
6. Service Management
NDIS Practice Standards:
1. Rights and Responsibilities 2. Provider Governance and Operational Management
Aged Care Quality Standards
8. Organisational governance

Related Legislation & References
Aged Care Act 1997 (Cth), Schedule 2 User Rights Principles 2014. Charter of Rights and Responsibilities – Home Care Aged Care Quality & Safety Commission Archives Act 1983 Australian Privacy Principles Children and Young Persons (Care and Protection) Act 1998 Commonwealth Home Support Programme Guidelines Commonwealth Privacy Act 1988 *Crime Commission Act 2012* *Independent Commission Against Corruption Act 1988* *Mental Health Act 2007* National Disability Insurance Scheme (Protection and Disclosure of Information - Commissioner) Rules 2018 National Disability Insurance Scheme (Provider Registration and Practice Standards) Rules 2018 National Disability Insurance Scheme Act 2013 National Disability Insurance Scheme Code of Conduct NDIS Quality and Safeguards Commission *Ombudsman Act 1974*

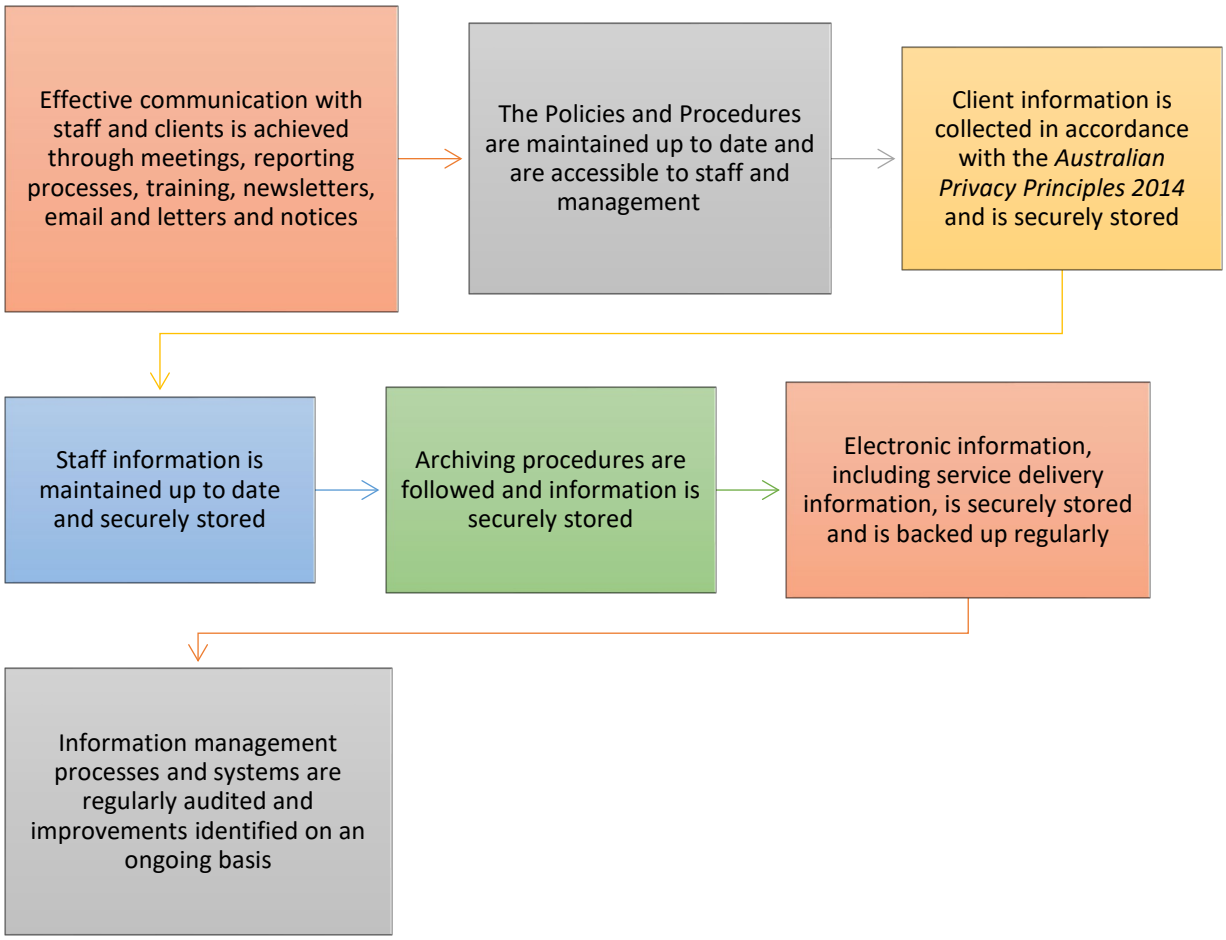
Privacy Amendment (Enhancing Privacy Protection) Act 2012 *Privacy and Personal Information Protection Act 1998* Privacy and Personal Information Protection Act 1998 *Public Interests Disclosure Act 1994* *State Records Act 1998* United Nations Convention on the Rights of Persons with Disabilities *Work Health and Safety Act 2011* *Workers Compensation Regulation 2010* *Workplace Injury Management and Workers Compensation Act 1998*

Related Procedures	
Section 2 – Regulatory Compliance	Section 8 – Physical Resources
Section 7 – Human Resource Management	Section 15 – Privacy and Confidentiality
Documents/Forms	
Minutes of staff, management, program, CCC meetings	Shared Drive
Client information	Client Management System (ProSIMS), shared files and paper files kept in locked files and compactus
Financial management records	CFO and finance team, shared files
Attendance sheets and Care sheets	Shared files and coordinator files

Responsibilities and delegations	
This policy applies to: Clients Employees/volunteers	**It will be distributed through:** Client handbook, Coastlink website, Coastlink brochures Employee/volunteer handbook, shared drive
Policy approval	Board

Definitions
Refer to Definitions list at front of Coastlink Policy and Procedure Manual and 3.7.8 of this document.

INFORMATION MANAGEMENT SYSTEMS PROCEDURE OVERVIEW



3.1 Communication Strategies

Underpinning the management of information in COASTLINK are the following communication strategies:

- Regular and structured management, staff and program meetings that involve all staff (see 1.7 Management/Staff Meetings)
- Regular Continuous Improvement Committee meetings are held so staff have input into new policies, procedures and forms as well as working with management to ensure continuous improvement across the organisation. (See Section 5 Continuous Improvement);
- Monthly or two monthly program meetings where new and reviewed policies, procedures, forms and other pertinent issues are discussed;
    - Training takes place at these meetings in new policies, codes of conduct, procedures and forms.
- Regular reporting (see 1.8 Management Reports);
- Regular information and training sessions for staff are used to communicate feedback, changes, client and carer information, health issues, clients rights and so on;
- Involvement of staff in the planning process (see 1.14 Planning);
- A quarterly newsletter for staff and clients (separate) prepared by the Coordinators/Admin including information on improvements implemented;
- Emails and memos to staff as required informing them of improvements and resultant changes, new policies, as well as staff issues and Board member profiles;
- Internal email addresses are provided to all new staff;
- On on-line system (TimeOnLine) provides access to all client information through their mobile phones or tablets;
- TimeOnLine also provides support worker access to their own personal information and rosters;
- All policies and procedures are available to staff through the Coastlink web page and TimeOnLine;
- Letters and notices to clients as required;
- Website staff portal for access to policies, procedures, newsletters, minutes and other information;
- An internal communication plan has been developed for use across the organisation.

3.2 Policies and Procedures Manual

3.2.1 Structure of the Policies and Procedures Manual

The COASTLINK Policies and Procedures include the following components:

- Care sheets filed in client files
- Internal emails
- Informal and formal meetings

Coastlink

Proposed SharePoint Format

Restricted Access

Index

- Human Resources
- Leadership
- Governance
- Finance Risk and Audit
- Compliance
- Information Technology

Common Access

Index

- Correspondence
- Clients
- Programs
- Meetings
- Policies and Processes
- Document Register
- Assets

The Policies and Procedures are maintained as read-only documents in the Common Drive and through the staff portal on the website, on TimeOnLine and in Hard Copy at every Coastlink permanent venue. They reflect relevant legislation, standards, funding requirements and sector policy.

The CEO through the Compliance Officer is responsible for maintaining the information up-to-date with assistance from the senior staff and other staff as required. The involvement of all staff is encouraged to ensure policies and procedures reflect practice and to foster ownership and familiarity with the material.

The Policies and Procedures Manual includes the following sections:

Introduction and Table of Contents

1. Corporate Governance/Financial Management
2. Regulatory Compliance
3. Information Management Systems
4. Community Understanding and Engagement
5. Continuous Improvement
6. Risk Management
7. Human Resource Management

7B Child and Young Person's Policies

8. Physical Resources
9. Service Access
10. Assessment
11. Support Planning and Delivery
12. Client Reassessment
13. Client Referral
14. Information Provision
15. Privacy and Confidentiality
16. Complaints and Client Feedback
17. Advocacy
18. Independence
19. Human Rights and Zero Tolerance
20. Accommodation Policy
21. Specialist Disability Accommodation
22. Support Coordination
23. Subcutaneous Injections
24. Catheter Care
25. Enteral Feeding and Management
26. Complex Bowel Care
27. Antimicrobial Stewardship
28. Pandemic Infection Control Policy
29. Business Continuity (live and focused on COVID response)
30. Ventilation

Forms

A copy of each form used by COASTLINK is maintained on the shared drive and in the Master Forms file (Document Register) maintained by the Compliance Officer.

3.2.2 Access to Policies and Procedures

All staff can access the Policies and Procedures through the shared terminals available to coordinators and office staff and located in off-site centres. If staff require a paper copy of procedures these can be requested from their supervisor but once printed are uncontrolled and should only be used as an immediate reference.

A copy of the policies and procedures manual is available via a staff only portal on the Coastlink website. A copy of the policies has been uploaded to TimeOnLine when the system is functionally available for this process.

Clients and their representatives can view the sections of the policies and procedures directly relevant to service delivery on a terminal by request. Staff can provide assistance if required.

3.2.3 Updating the Policies and Procedures

The CEO (through the Compliance Officer) is responsible for maintaining the policies and procedures up to date. The involvement of all staff in reviewing policies and procedures is encouraged to ensure they reflect practice and to foster ownership and familiarity with the material.

The Continuous Improvement Committee reviews any proposed major changes to existing policies or new policies for comment or suggested changes. Following policies and procedures are sent to the Board for approval (minor changes may be approved by the CEO as long as they do not affect organisational governance decisions, or impact on insurance arrangement).

The need to update the Policies and Procedures Manual, forms or other material may occur through:

- Changes in legislation or regulations
- Changes in funding or funding guidelines and requirements
- Feedback from staff, clients and their representatives/carers, other agencies etc.
- Management and Board decisions
- Adverse Event Reports
- Audits (of policies and procedures and responsive audits) and
- Reviews.

The process for updating the Policies and Procedures, forms etc. is:

1. When the need for changes is identified these are discussed with the CEO.
2. The CEO develops draft changes with the assistance other staff or delegates this task to other staff.
3. Draft changes are reviewed by senior staff and are taken to the Continuous Improvement Committee. The CEO decides if the changes need Board approval and submits them as necessary.
4. When changes have been approved by the Board the CEO updates the Policy and Procedures manual.
5. The Policy and Procedures manual is updated under the Management Folder including forms and the table of contents. Once updated and approved the policies are converted to PDF and saved under Policies and Procedures. Old versions are archived in the Archive folder.
6. Staff are advised of changes to the Policies and Procedures either through a staff meeting, an email, a memo or a training session or presentations. Clients are advised, as appropriate and necessary, through staff, the newsletters, letters or flyers.
7. Major changes are recorded as an improvement in the Improvement Plan (see Section 5: Continuous Improvement).
8. Major changes are reviewed after an appropriate time to ensure they have achieved the required outcome.

3.2.4 Review Minutes of management and staff Meetings

The CEO or delegated staff member reviews the minutes of all management and staff meetings for decisions that need to be reflected in the Policies and Procedures.

3.2.5 Control of the Policies and Procedures

- Electronic read-only copies of the Policies and Procedures material are accessible to staff including on the website and on TimeOnLine.
- Only the CEO can initiate changes to the original policies and procedures and only within the process specified in 3.2.3 Updating the Policies and Procedures.
- Printed pages of the Policies and Procedures can be made for staff to refer to but are uncontrolled documents once printed (other than the authorised printed copy/copies). These must be kept to a minimum. The Compliance Officer is responsible for recording the location of any full copies of the Policies and Procedures and for ensuring that they are updated when the originals are updated.

3.2.6 Review of Policies and Procedures

Policies and procedures including forms are reviewed over a 3 year period as documented in the Policy Review Schedule. This is described in detail in Section 5: Continuous Improvement.

3.3 Client Information

3.3.1 Principles for the Collection of Client Information

See Section 15: Privacy and Confidentiality.

3.3.2 Management of Client Information

Paper records

All clients have a paper file that includes referral information, assessment information, correspondence and any other relevant information. Paper files are stored in lockable filing cabinets in the head office or dedicated offices (i.e. Watanobbi). The Coordinators create new in-home notes and office files as required. Coordinators are responsible for filing and for securing the files and the storeroom.

In-home notes – Frail Aged

Clients who have in-home services also have a home notes file that includes information that Support Workers require access to, such as the support plans, Home Safety Checklist and consent form.

The Home Files are kept in a secure place in the client's home. If the client does not wish the home notes to be stored in the home (or if the notes are at risk of being lost or destroyed) arrangements are made for the staff delivering care to take the home notes into and out of the home each visit. It is essential for staff visiting the client's home, or providing other support outside of the client's home, to have access to the relevant support plans.

All other client files are kept in COASTLINK offices.

Creating a client file

The procedure for creating a client in-home/office file is:

- The Coordinator requests administration staff to create a home (for those receiving in-home service only) and office file following the assessment and acceptance of the person as a client.
- The in-home file is taken to the client's home either by a staff person who provides the first service or the Coordinator.

File storage and maintenance

- Files are stored in locked filing cabinets and compactus when not in use;
- All incoming correspondence is signed and dated by the Coordinator before being filed by administration staff;
- Keys to the filing cabinets are held by the Senior Finance Officer in a locked drawer.

File movements

To take a file out, the following procedure applies:

- The key is requested from the Senior Finance Officer;
- When the file is returned the compactus is locked and the key returned to the Senior Finance Officer;
- Files are never left on or in staff desks or anywhere else in the office overnight (unless in a locked room);
- Office-based files are never removed from the office without CEO approval; in-home notes files are returned to the office and filed with the office based file when the client ceases to receive support;
- Files for people who cease to access services are archived (see 3.6 Archiving).

Electronic records

Client information is also stored electronically on the client management system and in shared files on the computers. The Coordinators, Administration Assistants, Finance and administration staff are responsible for ensuring that data entry is completed (including entering a new client, amending data and exiting clients, setting up invoices and rostering clients with support workers).

3.3.3 Client Access to Information

See Section 15: Privacy and Confidentiality.

3.3.4 Support Service Information

Information on the support services delivered to clients is recorded on client management system and into shared files from recording sheets completed by support staff. The Coordinators are responsible for the entry of information and for the preparation of reports as outlined in 1.8 Management Reports.

3.4 Recording Service Delivery Information

The types of services provided by COASTLINK and recording instructions follow:

3.4.1 COASTLINK Programs

COASTLINK is a multi service provider. Details of the services provided are in Section 11.3.

3.5 General Information

Each program is responsible for organising and maintaining the filing of general information for their area of operation or where information is provided relevant to their clients.

3.5.1 Staff Records

Support staff files are kept in a filing cabinet in the office and are available only to the Coordinators and management. Management and office staff files are kept by the Human Resources Officer in locked files and are available only to the Senior Finance Officer, the Human Resources Officer and the CEO. The filing cabinets are locked when the office is unattended.

Staff access to staff files

Staff can access their files as per the procedures specified in 7.7 Staff Files.

3.5.2 Minutes of Meetings

Minutes of all Staff and Management meetings are maintained on the shared drive. Minutes of senior management meetings are to be stored in a secure partitioned section of the S drive, with access restricted to senior management only.

Board minutes area to be stored in the Restricted drive under the *Governance* sub folder which is only available to the CEO.

All Board papers (formal meeting papers provided to the Board for the purpose of director and committee meetings) including those with private notations are to be collected at the end of each Board meeting by the CEO. The CEO is shred all collected papers within seven days of collection. The CEO is not to read or share any private notations from the Board.

Board members may maintain their own private notations that are not written on a formal Board document.

3.5.3 Other Administrative Information

All other administrative information including funding information, financial information and general filing is maintained in the filing cabinets in the finance office. The cabinets are locked out of hours or when the office is unattended for a lengthy period of time.

3.6 Archiving

The Coordinators, Compliance Officer and administration staff are responsible for archive management. Archived files are stored in the archive storeroom. Archives are sorted by year and grouped as follows:

- Client records
- Staff records
- Administrative records including financial records
- Program information
- Policies and procedures.

All archived information is entered in the archives index. The index records the date of archiving, the file contents, the archive box name and number and the file number and date of destruction.

3.6.1 Timelines for Maintaining Records

COASTLINK records are securely destroyed after the following time periods:

Employment applications unsuccessful	6 months
Staff records	7 years after the staff person ceases employment
Client records	7 years after the client ceases receiving services except for Aboriginal and Torres Strait Islander clients, whose records are kept indefinitely and records of children aged under 18 years, whose records are kept until 7 years after they turn 18 years of age
Financial records	7 years
General administrative records	7 years
Policies and procedures	One year after each policy has been superseded.

3.6.2 Archiving Client Records

Client paper records

When a client leaves the service, their paper file is maintained in the client files for one year. After a year it is placed in an envelope and stored in client files archive box and entered into the archives index. Their name is also entered into the archive form for that box.

Client records are destroyed as per the timelines specified in 3.6.1 Timelines for Maintaining Records.

3.6.3 Managing Superseded Policies and Procedures

Whenever changes are to be made to the policies and procedures manual, or a form, the following procedure applies:

- Before making changes, copy the existing file into the Archive folder in the Policy and Procedures folder on the Shared drive.

Superseded policies and procedures and forms are destroyed as per the timelines specified in 3.6.1 Timelines for Maintaining Records.

3.7 Computers

3.7.1 Computer hardware/software

All Coastlink data is Clod based, through LoyalIT and Health Metrics (for ProSIMS data only), with all data stored in Australia;
COASTLINK uses Windows software and Office365 for email;
MYOB is used for financial documents and is a Cloud based system allowing access by Coastlink's External Financial Contractor;
ProSIMS electronic rostering system is used to roster all staff and is Cloud based;
Staff are allocated logons for ProSIMS at orientation. These are not to be shared at any time;
Coastlink uses ProSIMS as an integrated client management, rostering and human resources system;
ProSIMS provides access to staff private information, rosters and relevant client information via their staff member's mobile phone or tablet;
Laptops are provided to all office staff for access to the Cloud for all Coastlink information and systems;
Clients have access to computers at some of our centres which can be used for Internet and other use;
Senior manager and other coordinators are provided with Ipads and phones as needed to work on Coastlink business and to make access outside the office easier.

3.7.2 Data Storage

All COASTLINK data including clients, financial and administrative data, is stored in the Cloud in SharePoint. A Restricted section is only available to staff as identified by the CEO. It

includes Board, HR, IT, Compliance information, Finance, Risk and Audit information.
Programs will have access to their program budgets on the Common Drive.
All staff uses the shared files so non-confidential information can be shared.

3.7.3 Backups

All Coastlink data is stored in the Cloud. The Cloud provider is sourced through LoyalIT. They only store data in Australia.

Loyal IT has been engaged as COASTLINK's IT support and has organised a comprehensive back up system with the Cloud provider requiring no onsite user intervention due to the offsite backup system in place. All monitoring and health of backups are maintained by Loyal IT and as such, all responsibility is with Loyal IT

3.7.4 External Programs

No programs, external data or utilities are installed onto any workstation without the permission of the CEO. Installing programs or other external data or utilities can introduce viruses into the workplace and can cause serious problems with the computer system.

MyAgedCare website is used to manage CHSP client referrals and activities;

The Commonwealth Data Exchange (DEX) is used to report CHSP activities;

The NDIA portal PRODA is used to manage NDIS participant information and Coastlink's NDIS activities;

AUSkey is required for access to the MyAgedCare, DEX, PRODA, BNG NGO Services Online and ORIMA websites. It is installed on the computer of the CEO and Operations Manager and coordinators requiring access to Commonwealth controlled systems.

3.7.5 Passwords

Staff are assigned logon credentials by the Human Resources Officer.

When a staff member is on leave, has been suspended or is generally unable to access his/her computer, Coastlink will access their emails as a way of ensuring continuance of normal business.

3.7.6 Email

Email Use Policy – to be signed by each person who has access to email

Communications through Coastlink electronic mail (email) system is exclusively intended for business communication and to support the organisation's objectives.

This policy sets out what Coastlink considers is acceptable use of the Coastlink's email system.

All staff are allocated an email address. They are password protected through Microsoft Office365 security settings and monitored by LoyalIT. Support workers are only able to access internal emails through their account (both to send and receive).

Policy Objectives

1. To provide email to facilitate business communication and to enhance productivity. Personal use of any kind is not allowed.

2. To ensure that best practice is followed in the use of, access to and distribution of email and its proper use by all staff members.

3. To ensure that all electronic records are documented to provide a formal record in accordance with Coastlink current file management system.

Email : Use Protocol

The purpose of this document is to establish a best practice email protocol that will provide guidelines on the use of, access to, and disclosure of email, including internal email, and its proper use by all staff. This protocol will be kept up-to-date as developments occur in the management of e-mail.

Email : Corporate Records Management

Email messages and their attachments are corporate records, as they serve to document Coastlink's business activities and therefore need to be retained within the corporate records management system as evidence of those actions.

Coastlink's documentation is a continuing record of how business has been conducted since the inception of the business. Email records are part of this record and must be filed accordingly.

Email messages consist of two components

i Message Envelope (Addressee, sender, routing details, date and time sent)
ii Message Body (text of message, including signature block and attachments)

Coastlink is obliged to keep full and accurate records of its corporate business activities. In the case of email, the integrity of the corporate record depends on these two components being maintained as a whole. Incomplete messages will fail to act as reliable evidence of the business activities that they document.

Additionally the business context in which the e-mail occurred must be retained. This refers to related messages in that particular interchange of messages.

Email messages, like records in other formats are subject to legislation such as the Australian Privacy Principles, the Freedom of Information Act 1989 and legal processes such as discovery and subpoenas. The records may also be required by Royal Commissions, the Courts, auditors and others.

All external email messages (regardless of how important they appear) need to be maintained or electronically archived so that there is a convenient and continuing record of all correspondence related to the topic.

For incoming email, if a staff member is the only recipient, or the first person on the distribution list, that person is responsible for registering, securing, filing the email so other staff can access it if relevant.

For external email, the person who sends the email is responsible for registering its electronic filing.

For any response to an internal email, the responder is responsible for its filing.

Filing of emails is only required where access is necessary for other staff, the Board or where business processes require a hard copy.

Access Rights

Access and use of email facilities is strictly limited to designated users and must not be extended to any other person.

Access to email is approved using the same process for arranging access to Coastlink's network systems. Business need must be established and manager authorisation is required.

Access is password protected.

Only the external support company can change the email settings or rules which govern the email system at Coastlink. If there is an issue with email such as mail getting stuck in the outbox the matter is to be referred to the system administrator.

Appropriate use of E-mail

Email is not a replacement for the corporate document management system.

Email may be used for the same communication purposes and under the same Code of Conduct as the mail service, facsimile, hand-delivery, the telephone, and face-to-face conversations and meetings.

E-mail users are expected to use reasonable judgement in the performance of their duties.

Some of the uses that are best adapted to e-mail communications include:

- Forwarding correspondence
- Replying to e-mail correspondence
- Scheduling meetings or other events without playing “phone tag”
- Distributing professional meeting agendas, minutes
- Distributing professional group information through discussion groups and networks
- Distributing bus lists and shift confirmation from field workers
- A quick means of communication with other community service agencies that do business with Coastlink.

Communication Standards

When using email, follow standards you would use in normal business communications when communicating with clients and customers, ie, use the corporate standard for letters and language, and appropriate email communication. See the Email Communication Guide at the end of this document.

Monitoring of E-mail

It is essential that the CEO be fully informed of all important correspondence that enters and leaves Coastlink. Copies of all email relating to funding or funding providers must be forwarded to the CEO.

Inappropriate Use of E-mail

E-mail and the Coastlink computer networks that support it are a company asset. Like any company asset, they are to be used exclusively for Coastlink business.

E-mail is subject to the same legislative requirements, policies and practices that apply to written and verbal communication, such as the Sex Discrimination Act 1984, Disability Discrimination Act 1992, Racial Discrimination Act 1975. Employees should note that they

may face the prospect of criminal charges for sending offensive, harassing, discriminatory, pornographic, sexually explicit or racially vilifying messages.

The following uses of Coastlink e-mail are never appropriate and are prohibited.

- Illegal or fraudulent activity.
- To create, send or copy offensive, harassing, discriminatory, pornographic, sexually explicit, racially vilifying messages, chain emails.
- To receive, download or send copyrighted materials, trade secrets, proprietary financial information or similar materials without prior authorisation.
- To solicit or promote commercial ventures, religious or political causes.
- The release of untrue, distorted or confidential information regarding Coastlink business.
- To introduce computer viruses and the like into the Coastlink network system.
- As a forum to criticise Coastlink, management or co-workers. The nature of emails means that they are not easily destroyed and are very easily disseminated
- "Spoofing", ie, constructing an email communication so it appears to be from someone else.
- Attempting unauthorised access to e-mail or attempting to breach any security measures on any email system, or attempting to intercept any e-mail transmissions without proper authorisation.
- To present an email message in such a way that it may be interpreted by a recipient as official correspondence when it is not.
- Giving advice on Coastlink business outside area of expertise.
- Transacting Coastlink business when not authorised to do so.

Responsibility of the CEO

- Informing employees of any changes in legislation regarding email.
- Taking appropriate action against inappropriate use of email by employees and enforcing the policy.
- Maintaining a complaint history that may indicate patterns of behaviour by employees in regard to email use.

Disciplinary Action

Disciplinary action, according to Coastlink's Disciplinary Procedures, up to and including dismissal, may be taken against any Coastlink email user found to be using the e-mail system in a manner that is in contradiction to, or in violation of, this policy.

Anyone suspecting misuse, or attempted misuse, of email is responsible for reporting such activity to the Manager.

Creation and Transmission

Providing warning notice such as “Confidential Communication – Do Not Forward” does not guarantee confidentiality. It does not preclude the recipient from forwarding it to another party. Likewise, a court may later find that a document is subject to public disclosure despite its “confidential” designation.

Email is retrievable long after one “deletes” it from a computer. Recipients may save, print or forward the message. Computer backup systems may store electronic data in retrievable form for long after the user hits a “delete” key. Coastlink has an external backup system which keeps records of all electronic transactions for at least 7 years.

Email is not an appropriate medium for large document communication that can slow or halt the e-mail network. Avoid also sending excessively large attachments for the same reason. Large documents may be better to be sent by post.

Responsibilities and Maintenance

- Follow procedures as outlined in this protocol, for corporate records retention.
- Mail should be checked regularly and replied to appropriately in priority order.
- Where a person is absent for a period, arrangements MUST be made to establish a delegate to read their e-mail (refer to e-mail training documentation).
- When commenting/replying, include the original text as part of your response, thereby creating a meaningful and contextual record.
- Do not alter the email record in any way.
- Regularly archive business emails then delete from Outlook. E-mail is not a replacement for the corporate document management system. This maintenance will reduce the storage burdens, ensure that adequate storage exists for incoming messages, and improve the overall performance of the system. People should aim to maintain a mailbox size of less than 50MB. Limit the size of attachments. Large attachments have a significant effect on system performance and should be kept to a minimum.
- Access and confidentiality. Email users should NOT assume that their communications are confidential or private. Email users should exercise great care in using email.
- Disclaimers. The organisation’s email system automatically includes a DISCLAIMER in the footer of every email transmission.

Email Use Agreements

Prior to being granted access to Coastlink’s email facilities, employees will be provided with a copy of this Protocol and will be required to sign an Electronic Mail Use Agreement that acknowledges compliance with the protocol.

The Electronic Mail Use Agreement appears as an addendum to this policy.

Email Communication Guide

- Know your audience
- Proof-read, re-read your mail before you send it
- Keep messages brief and to the point
- Use appropriate business style and language when communicating formally
- Be wary of the use of informal language. The nature of email lends itself to informality, but language taken out of context can be injurious to individuals and the organisation. Rule of thumb: if you would be unwilling to have the message published, do not send it.
- Do not over-distribute messages; only post messages when they are relevant
- Respect the privacy of others; and don't be fooled by illusion of privacy
- Be aware of differences in email systems, particularly problems associated with sending attachments
- Cite appropriate text and references in responding to a particular event, topic, or issue
- Separate opinion from non-opinion
- Respect copyright and license agreements
- Do not mark messages URGENT unless they really are
- Avoid all CAPS. This is considered to be shouting
- Be careful what you say about yourself and others
- Do not overuse "Reply to all"
- Do not abuse others, known as "flaming", even in response to abusive communication
- Do not send unsolicited, typically unwanted broadcast messages, known as "spam" to anyone.

Electronic Mail Use Agreement

I, …… have received and read Coastlink's Email Use Policy and agree to comply with all provisions and terms stated in that document.

I understand and acknowledge that my use of e-mail and facilities will be monitored according to the guidelines outlined in the Policy.

I understand that failure to adhere to the Policy may result in disciplinary action, up to and including dismissal.

SIGNED: …….

DATE: …….

3.7.7 Internet AND COASTLINK PHONES

Internet access and Coastlink owned phone use is restricted to work related purposes unless stated otherwise in an employee's contract.

Internet access reports are maintained and can be regularly reviewed by the CEO.

Under no circumstances are staff to access pornographic or sex related sites and doing so will lead to disciplinary procedures including dismissal.

3.7.8 SOCIAL MEDIA POLICY

The use of social media has increased dramatically over recent years. This policy is designed to guide staff members in their use of social media when posting any matter which may concern COASTLINK, its clients and their families, other staff members and any other stakeholders in the Company.

Definitions

Identifiable personal use: Use of social media where a staff member can be identified as an employee of COASTLINK. The identification may be though means such as the staff member's social media name, character, profile or comments.

Social media: Online media designed to allow information to be shared and disseminated and created using highly accessible and scalable publishing techniques. Social media services include, but are not limited to:

- social and professional networking sites (eg Facebook, LinkedIn, Myspace, Bebo, Yammer)
- geo-spatial tagging (FourSquare)
- blogs, including corporate blogs and personal blogs
- micro-blogging (eg Twitter)
- video and photo sharing websites (eg Flickr, Youtube)
- blogs hosted by media outlets (eg 'comments' or 'your say' feature on theage.com.au)
- wikis and online collaborations (eg Wikipedia)
- forums, discussion boards and groups (eg Google groups, Whirlpool)
- vod and podcasting
- online multiplayer gaming platforms (eg World of Warcraft, Second life)

- instant messaging (including SMS)
- any other social media platforms not specifically names in this policy.

This procedure covers the use of social media by any means including using any computer, tablet, mobile phone or handheld device either Company owned or privately owned by staff members.

Staff member/employee: a person employed by the COASTLINK who has a permanent, casual or temporary contract.

- No employee is permitted to be connected on Social Media with clients, families of clients, or carers;
- All Coastlink related Social Media activity by employees should be directed through the official Coastlink Facebook page.

Accessing Social Media

When staff members access social media either in the workplace or outside it they have responsibilities to ensure that:

- COASTLINK clients, their families, other staff members, including managers and Directors, are not defamed.
    - This includes posting racist, sexist or personal remarks as well as any gossip or rumours of a personal nature aimed at any Company stakeholder including other staff members.
- material posted by a staff member does not mention the personal lives of others including other staff members, clients or other stakeholders.
- any information posted does not include any confidential information regarding any aspect of COASTLINK business including matters concerning clients and other staff members.
- information that may be considered to be COASTLINK intellectual property or which may give a competitive advantage to a competitor is not posted.
- information is not posted which brings COASTLINK into disrepute.
- material posted does not bully, intimidate, harass or belittle COASTLINK stakeholders including clients and other members of staff.

Note: COASTLINK does not condone any illegal activities carried out by any staff member on any social media site at any time.

It is important that staff members consider the impact their online activities can have on their employment. COASTLINK requires employees to abide by this policy at all times.

- Staff members should be aware that failure to abide by this policy can lead to disciplinary action up to and including termination.

3.7.9 computers and hand held devices- Getting Help and Reporting Problems

COASTLINK maintains an ongoing support agreement with Loyal IT to maintain the COASTLINK computer system. This includes software installation and updates and monitoring backups.

If a staff member experiences any problems with a program or computer or other piece of equipment they can, in the first instance, contact the Human Resources Officer who, if necessary, will ask Loyal IT to provide assistance.

3.8 Notifiable Data Breaches

3.8.1 WHAT IS A MANDATORY DATA BREACH NOTIFICATION?

There is a formal legal requirement to provide notice of any serious breach to affected individuals to the Privacy Commissioner and a process to be implemented to investigate and deal with such breaches. Storage of personal information of any kind has strict obligations under the Privacy Act not to disclose that information to third parties. If there is a breach by employee by error, system glitch, third party theft or cyber-attack it may need to be reported.

3.8.2 DO ALL DATA BREACHES REQUIRE NOTIFICATION?

Not all data breaches will require notifications. In order to trigger the notification requirement the CEO would need to conclude that there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by the entity, and this would likely result in serious harm being caused to any of the individuals to whom the information relates.

Serious harm, in this context, could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.

In deciding whether a breach '*will likely result in serious harm*', entities are required to have regard to a list of relevant matters outlined in section 26WA of the act. Such matters include the kind of information leaked, the sensitivity of the information, the kind of persons who may have obtained the information and whether the information has been otherwise protected.

Without limiting the effect of the Act, things like credit card or account details and medical information are likely to give rise to the risk of harm.

If the CEO believe there are reasonable grounds to suspect there may have been an eligible data breach, then the CEO or Senior Management must carry out an expeditious and reasonable assessment within 30 days. If such a breach is found to have occurred then, unless an exception applies, you must as soon as reasonably practicable prepare a statement to give to the Commissioner, and must take all reasonable steps to notify each of the individuals whose information has been breached.

3.9 Monitoring Information Management Processes and Systems

Information management processes and systems are regularly audited as part of the COASTLINK audit program and staff, clients and other stakeholders are encouraged to provide ongoing feedback on issues and areas where improvements can be made (see Section 5: Continuous Improvement).