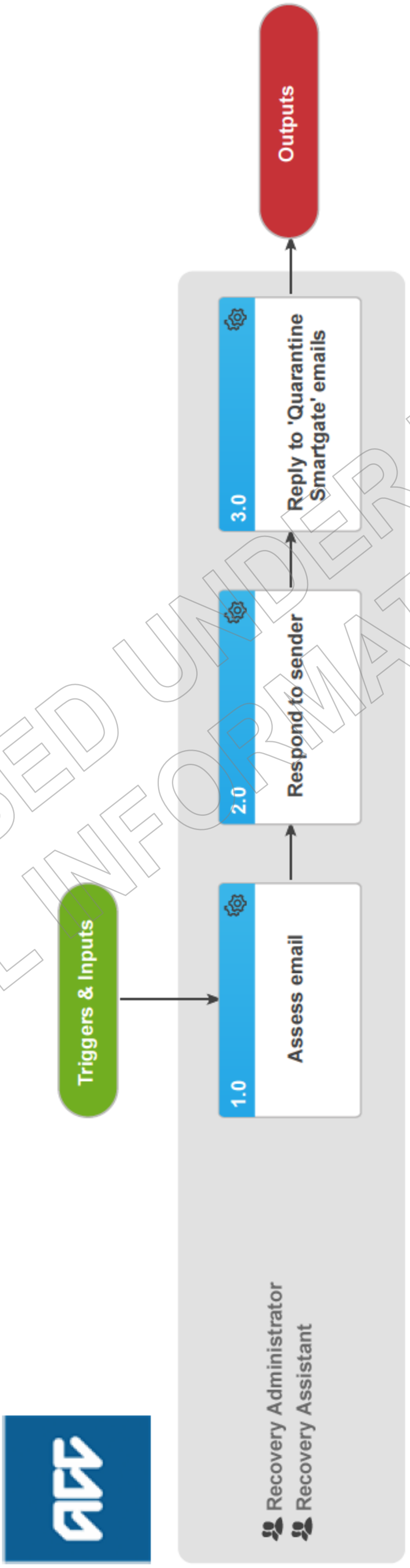
(NGCM) Complete Inbound Client Related Emails (Shared Inbox) v32.0



(NGCM) Complete Inbound Client Related Emails (Shared Inbox) v32.0

Summary

Objective
To assess and complete email requests that are received in a shared inbox so that we can respond in a timely, consistent way.

Owner Paul Harvie

Expert Peter Bennett

Procedure

1.0 Assess email

Recovery Administrator, Recovery Assistant

a In Salesforce, set your status as 'Available for work'. This will allow you to receive the next priority email task.

NOTE What can you view in Salesforce?
• The latest email received will display in the email message.
• Any attachments relating to the latest email will display in attachments.
• Additional emails relating to the chain will show under Email message. You can also see if there are any attachments with the additional emails.

NOTE What if the email task is for a 'Quarantine Smartgate' message for an outbound email?
Go to Activity 3.0 Reply to 'Quarantine Smartgate' emails

NOTE What if the email was sent to the incorrect email address?
Please forward the email to the correct shared e-mail address. The team that should have received the email in the first instance will file away and create the required tasks.

NOTE What if you receive an ACC179 for Long Term or Extended Nursing Services?
Forward the email to claimsdocs@acc.co.nz. Delete the email from the shared inbox. In Salesforce close the associated email task. This process ends.

b Select [Copy Search] and copy this into the search box of the shared inbox you are working in. Choose [All Mailboxes] to search the entire shared inbox, then open the related emails.

NOTE What if the copy function doesn't work?
Search the inbox using the client's claim number, client's name, email address to locate the email.

NOTE What if I'm a Recovery Administrator and I locate the email I've been tasked with?
Categorise your email as 'Currently Being Worked On'. If you find your email and it already has a category, Mark Closed your task in Salesforce.

NOTE What if I'm a Recovery Assistant and I locate the email I've been tasked with?
Tag as "Managed by Recovery team, using the categorization function within Outlook. Complete the request, delete the email and close your task in Salesforce.

NOTE What if you locate another email relating to your client, but it's not allocated to you in Salesforce?
When you have completed your current piece of work and then located an additional email related to the client:
1) Tag email as 'Managed by recovery team'
2) Complete the request
3) Locate the email task in Salesforce by searching for the email address via the global search box
4) Close the email task
5) Delete the email from the shared inbox

c Perform the relevant inbound privacy checks on the inbound mail.

NG SUPPORTING INFORMATION Inbound and Outbound Document Checks

d Check if the file size of any documents attached exceeds 10MB.

NOTE What if I am a Recovery Assistant and have identified documents that exceed 10MB?
Depending on your geographic location, forward the email to the Inbound Document Management team in Dunedin or Hamilton, requesting them to upload the document to the client's claim. IDMT will file away the email once it has been actioned.

• DMTDunedin@acc.co.nz
• DMTHamilton@acc.co.nz

NOTE What if I am a Recovery Administrator and have identified documents that exceed 10MB?
Use Adobe Pro to
Reduce file size:
• Select Optimize PDF
• Select Reduce File Size
Or
Split document
• Select organize page
• Select Split
• Select Split by File Size (up to 10MB)
The document will save in the same location and the original document and will be name PART1, PART2 (depending in the size of the file being split).
Documents are ready for uploading.

2.0 Respond to sender

Recovery Administrator, Recovery Assistant

a Review the email to determine what action is required

NOTE What if no response or action is required?
Some emails will be sent to the shared inbox as an auto reply or a 'Thank you'. These emails will create a task in Salesforce however there is no action or response required. For these emails, close the task and delete the email. Air New Zealand itinerary confirmation emails, are forwarded to the client as part of the arrange flights process therefore, the tasks need to be closed and emails deleted in this instance too. This process ends.

NOTE **What if the email is a verification of email address?**

If the verification is for a client email address:
• File away the email
• Update the party record with the verified email address

If the verification is for a client's employer?
• Open the party record and file away the email
• Add the employer as a contact person via the "Contact Person" tab

NOTE **What if the email is for an invoice query?**

Go to the '(NGCM) Resolve Invoice Queries process.

PROCESS (NGCM) Resolve Invoice Queries

NOTE **What if no response is required, but action is required?**

Complete the required actions(s) of the email.

NOTE **What if there is an action that I don't have the delegation to complete?**

Determine who can complete the action and forward the email to an individual or team. Delete the email from the shared inbox. In Salesforce click 'Mark Closed' the associated email task. This process ends.

b File away the inbound email. If the email does not have a document attached, file away to the client's Recovery Plan using your individual email address. If the email contains a document, it must be filed away to the ACC45.

NGCM Filing Away - System Steps

NOTE **What if you cannot locate the claim in Eos?**

Reply to the email requesting additional information from the sender. As this email cannot be filed away, move it from the 'sent items' folder in your Outlook mailbox to the 'Deleted Items' folder in the shared mailbox. This will allow the next person to respond once a reply is received.

NOTE **What if you identify a Provider has sent several emails with documents attached for a single claim?**

Contact the Provider to understand the issue. It may be due to size restrictions on their email server. If this is the case, request the Provider uses the same subject line in all emails relating to the single claim.

NGCM Filing Away - System Steps

c Check that the email has successfully filed away. Once you have viewed the email on the claim (this could take up to 5 minutes), delete the email from the inbox and update the document properties of the email in Eos.

d In Eos, update the description field of the email contact using an easily identifiable description.

NOTE **What if there is an action that needs to be completed by a Recovery Team member in the email?**

Create a NGCM Action Attached Request Task and assign to Assisted Recovery or Recovery Team member.

NOTE **What do you do if filing away is taking too long?**

• Log a ticket with ICT via the desktop application.
• Create a NGCM - Follow up Report/ACC Request in Eos.
• Update the task description to show [Check Email] and include the [Copy Search] string from the Salesforce task. Include any other relevant information..
• Leave the email in the shared inbox and categorise as blue. Do not create folders
• Mark Closed the task in Salesforce
• Go available to receive your next piece of work.

NOTE **What do you do if you receive a NGCM - Follow up Report/ACC request task?**

Check the claim to see if the email has been filed away.
If it has:
• Update the properties of the document
• Action the appropriate task in Eos for the Recovery Team (eg Follow up task). If there is no follow up task on file and we've received a report, create a NGCM Action Attached Documentation task.
• Go to the inbox and search for the email using the 'Copy Search' string and delete the email.
• Mark Closed the task in Salesforce.
• Go available to receive your next piece of work.

If it hasn't:
• Go to the inbox and search for the email using the 'Copy Search' string.
• File away the email.
• Return the task to the queue in Salesforce, update the description to 2nd file away (etc) and change the due date to the next business day.

e Action the appropriate task in Eos for the Recovery Team (eg follow up task).

NOTE **What if the document received is an ACC18 medical certificate?**

Create an NGCM - Action Medical Certificate task and link to the ACC18. The task will automatically route to Assisted Recovery or Individual managing the claim.

NOTE **What if there isn't an associated task for this document?**

Create a NGCM Action Attached Documentation Task and assign to Assisted Recovery or Recovery Team member.

f Respond to the sender. Ensure you are familiar with the ACC guidelines for communicating with customers before responding.

NG GUIDELINES Customer Communication

g Perform the relevant privacy checks before disclosing information.

Privacy Check Before Disclosing Information Policy

h File away the response email to the client's Recovery Plan using your individual email address.

NOTE **What if I am a Recovery Assistant and I have not completed all actions related to an email at the end of the day?**

• File away the email using your individual email address and delete the email from the inbox.
• Update the Recovery Plan with progress to date.
• Create follow up action tasks (Reminder actions or Contact actions) for further actions required with a due date.

Recovery Plan - Create Reminder Actions - System Steps

i Delete the inbound email from the shared inbox

j In Salesforce, Mark Closed the task.

k Go available to receive your next piece of work.

3.0 Reply to 'Quarantine Smartgate' emails

Recovery Administrator, Recovery Assistant

a Open the original email and perform the outbound document dispatch checks. Refer to the 'Inbound and Outbound Document Checks' document below. For further information refer to the Quarantine Email guidelines.

NGCM - Quarantine Email guidelines

NG SUPPORTING INFORMATION Inbound and Outbound Document Checks

NOTE **What if I receive a Salesforce Task to review a quarantine email?**

When reviewing the quarantine email, open the EOS email contact and add your initials and the Salesforce Task ID (T-XXXXX).

NOTE **What if I am a Recovery Assistant and identify an error?**

• Call or message the person who created the email to discuss the error you have found
• Find contact related to that email in Eos, Edit the contact and add “PLEASE DELETE”
• Delete the quarantine email
• Open the related claim, fix the error you have identified and resend the email
• Email your Team Leader to delete the contact you have marked as “PLEASE DELETE” and ensure any documents attached to that email are also deleted from the contact.

NOTE **What if I'm a Recovery Assistant and identify a potential privacy breach?**

• Email your Team Leader to alert the potential privacy breach immediately
• Call or message the person who created the email to discuss the error you have found
• Find contact related to that email in Eos, edit the contact and add “PLEASE DELETE”
• Delete the quarantine email
• Open the related claim, fix the error you have identified and resend the email
• Email Team Leader to delete the contact you have marked as “PLEASE DELETE” and ensure any documents attached to that email are also deleted from the contact.

NOTE **What if I am a Recovery Administrator and identify an error?**

Email Recovery Team Member who generated the outbound response, requesting the error is resolved and the email resent.

Delete the quarantine email from the folder. For further information refer to the Principles Working in the Administration Team document.

NG PRINCIPLES Working in the Administration Team

When to save emails in Eos v7.0

Summary

Objective
If the client sends an email regarding a specific claim, upload it as a 'Contact' to that claim, otherwise upload it to Party level.

Uploading emails to the appropriate Party record:

• enables us to gather information more easily if the client re-quests a review or appeal
• provides a date and time stamp
• provides context for the email
• helps us manage requests from clients for their personal infor-mation
• provides greater integrity and accuracy of information
• provides a complete and accurate record of our contact with the client or party.

Owner John Sullivan

Expert Iosef Sengson

Policy

1.0 Rules

a You must upload all correspondence to the appropriate Party record in Eos, including emails to and from a client, provider or employer. This includes:

• general correspondence regarding our processes
• specific information about how we manage claims
• correspondence about the active management of a particular claim.

Emails saved in Eos must be a complete record of correspondence with the client and include:

• the date and time it was sent
• the name of the sender and the receiver.

You must save all appropriate emails into Eos, regardless of the number of emails sent and received on a topic. See:

• CHIPS process - File an inbound email to a party record or claim in Eos
• Eos Online Help - File an inbound email

You must secure all legally privileged information after uploading it to prevent the documents from printing when someone asks for a copy of their claim file.

Verifying and re-verifying an existing vendor, pro-vider or facility work email address
http://thesauce/team-spaces/chips/providers-vendors/provider--vendor-registration/process/verifying-an-existing-vendor--provider-or-facility-work-email-address/index.htm

File an inbound email
http://thesauce/team-spaces/eos-online-help/contact/email-toolset/file-an-inbound-email/index.htm

Email and Instant Messaging Policy
http://thesauce/resources-and-tools/policy-legislation/corporate-policies-a-z/email-and-instant-messaging/index.htm

2.0 Exceptions

a The attached table shows which email communications you are not required to save into Eos. If you're not sure whether to save an email into Eos, talk to your team manager.

If the source is...	then you don't need to save...

internal	• information relating to an ACC investigation
	• legally privileged information, including:
	  • any correspondence between ACC offices and ACC Legal Services
	  • any advice from ACC Legal Services
	• information from Government Services regarding:
	  • the Ombudsman, Privacy Commissioner or Health and Disability Commissioner
	  • a complaint
	  • ministerial correspondence
	• allocations, spreadsheets or dual management lists
	• requests for claims management staff, with the correct delegation, to reopen a claim
	• duration tool and case list filters
	• meeting invitations to discuss claim-related information
	• team manager coaching notes related to specific claims
	• lists of claims for panels

external	• information requests about provider claims
	• requests for information from providers about:
	  • claim details required to facilitate client treatment and invoicing
	  • the progress of any prior approvals for treatment
	• vendor enquiries about invoice payments for client services

Exceptions - Email in EOS.PNG

File an inbound email

Use these instructions to file an inbound email as an email Contact in Eos

Contact [redacted] **Last review** 09 Nov 2018 **Next review** 09 Nov 2019

How to: File an inbound email

Contacts are used to record details of communications with external parties, such as emails, phone calls, letters and faxes. It is important to record contacts so that other staff members are able to see all of the communications relating to a Claim or Party.

Email Toolset enables an incoming email to be forwarded to Eos, which creates an Email Contact. If the email has an attachment, it will also be visible in the Documents tab.

File an Outlook email as an Email Contact

You can choose to file an Outlook email to an Eos Claim and Party or to a Party only. The Email Contact must always be associated with a Party. If the Claim is sensitive, the Contact will only be visible at Claim level and not visible on the Party.

Step 1

Open Outlook and click '**Forward**' in the email you want to save as a Contact in Eos.

Step 2

Type the Claim number and/or ACCID in the '**Subject**' line as shown in the following table.

Type of filing	What to type in the 'Subject' line	Examples
Claim and Party	The Claim number and ACCID are both required	CLAIM: 10023858 ACCID: 10218672
Party only	The ACCID is required	ACCID: 10218672
Provider Party	The ACCID must be prefixed by 'PROV-'	ACCID: PROV-10FKAE
Vendor Party	The ACCID must be prefixed by 'VEND-'	ACCID: VEND-AA4435

Note:

- Customer numbers must be preceded by the phrase ACCID: followed by the Party ID
- Claim numbers must be preceded by the phrase CLAIM: followed by the Claim number.

Step 3

Check whether the **body** of the email contains an image, eg a signature logo. If it does, then you'll need to format the email as 'Plain Text' by completing the following:

- go to the 'Format Text' tab
- select 'Plain Text'
- the 'Microsoft Outlook Compatibility Checker' message will pop up
- click 'Continue' to format the email in plain text.

If you don't format the email as 'Plain Text', Eos will save the image and email as a separate document when you have complete 'Filing Away'.

Step 4

Enter the filing@claims.acc.co.nz email address as the 'To' recipient.

Step 5

Click 'Send' in Outlook.

The email will be saved in Eos and visible in the **Contacts** tab.

Note: If the email has an attachment, the attachment will be displayed as a hyperlink. Attachments will also be automatically saved under the **Documents** tab.

Back to top

Find an ACCID

If the subject line of the inbound email has not already been populated with the ACCID, locate the correct record in Eos.

To find the ACCID of a Party:

Step 1

Conduct a privacy check of the content of the email and attachments to ensure the information is relevant and appropriate to upload to Eos.

Step 2

Open the **party record**.

The number displayed at the top left hand corner of the Eos screen is the ACCID.

Step 3

Copy and paste this number into the 'Subject' line and type 'ACCID:' before it.

Back to top

Find a Claim number and ACCID

If the subject line of the inbound email has not already been populated with the Claim number and ACCID, locate the correct record in Eos.

Step 1

Conduct a privacy check of the content of the email and attachments to ensure the information is relevant and appropriate to upload to Eos.

Step 2

Open the claim.

The Claim number and ACCID will be shown at the top of the screen.

Step 3

Copy and paste the Claim number and the ACCID from Eos into the 'Subject' line of the email you wish to save as an Eos Contact.

Back to top

Promote a document to a Claim or Party

If an Email Integration Contact has an attachment, the 'Promote document' icon will be displayed next to it. This means you can add a copy of the document to a Claim or Party.

Step 1

Conduct a privacy check of the content of the email and attachments to ensure the information is relevant and appropriate to upload to Eos.

Step 2

Open the claim or party record and go to the **Contacts** tab. Click **Promote document**.

The 'Copy Attachment' window displays.

Step 3

Click the **magnifying glass** (search icon) to search for a Claim or Party.

Step 4

Enter your search criteria and click **Search**.

Step 5

Select the Claim or Party you want to attach a copy of the document to.

Step 6

Click **Copy.**

The document will be copied to the selected Party and/or Claim.

Back to top

Email and instant messaging policy

Contact Selwyn McCallum Last review 02 Dec 2019 Next review 01 Dec 2020

Policy statement

We use emails or instant messages to communicate, collaborate and share information.

When sending, or receiving emails or instant messages, we must uphold the reputation and standing of ACC in accordance with the Code of Conduct.

Objective

This policy outlines key principles for ensuring that emails or instant messages are managed in accordance with business needs, good information management practice and relevant legislative requirements.

Scope

This policy applies to all emails (including email attachments) and all instant messages that are created, sent or received through an ACC approved and provided system (eg Skype for Business). These messages and emails include all those created, sent, received and managed when acting for, or on behalf of, ACC.

Policy principles

We use ACC Email and Instant Messaging primarily for business purposes.

We may use email and instant messaging tools for limited personal use but must comply with the ACC Code of Conduct and Information Security policies.

The following use of email and instant messaging is not allowed:

- sharing of racist, sexist or inappropriate jokes
- sharing of emails or instant messages containing large and/or potentially malicious files (games, executable files, large videos) that can slow or destabilise our system
- sending of inappropriate emails and/or messages that reflect discrimination, bullying or harassment.

We are all responsible for effectively managing email and instant messaging tools to communicate, collaborate and share information internally and externally.

- Instant messaging is used for informal, short-term conversations.
- All emails or instant messages representing ACC's interests must be sent from an official ACC user account – firstname.surname@acc.co.nz.
- All emails and instant messages sent or received using ACC user accounts and systems are the property of ACC and must be treated as such.
- The email and instant messaging code of practice serves as a guide for appropriate behaviours in sending emails and messages.

Instant messaging and email systems must not be used as a system of record for storing ACC business decisions or business records.

A system of record is the authoritative data source for a data element or data entity. Email and Instant Messaging systems must not be used for the long-term storage of ACC business records.

A document is an ACC business record if:

- it contains information to help you carry out your work
- it has been used in your work to make a decision
- it reflects a business decision, or demonstrates an influence on a business decision
- you are required to act upon it
- it needs to be reported to another person or internal (or external) body
- it is proof of ACC's business processes
- it approves or authorises an action
- it signifies a policy change or development
- it relates to a significant ACC project or activity
- it helps other ACC staff to easily locate and trace the development of policies, decisions, procedures etc.
- it sets a precedent.

You may document a decision, or action, via email but must store that email/email thread in Eos, the shared drive, Document Store or similar. Do not keep the message in a folder in your Outlook account.

All email and instant messages are legally discoverable and may be requested as part of information requests arising from the Official Information Act, Privacy Act, Public Records Act or other legislative requirements.

We dispose of Email and Instant Messaging content according to legislative requirements.

Emails and instant messages must be managed in accordance with our approved Disposal Authorities.

Where an email that contains a business decision or action has been saved into a system of record as per 4.3 above, the original email can then be deleted.

Email and Instant messages must be available for retrieval and remain accessible for business and legal purposes up to the point of disposal.

4.5 We do not use unapproved instant messaging applications within ACC.

- Use of unapproved applications is a breach of ACC's Code of Conduct and may result in disciplinary action
- To confirm whether the application you are using is approved, contact the Information Security team.

Accountabilities

The Manager Information and Digital Tools with assistance from the Chief Information Security Officer (CISO) is responsible for this policy being implemented on behalf of the Chief Technology and Transformation Officer (CTTO).

Responsibilities

All staff are collectively responsible for Information Management at ACC.

Role	Responsibilities
Employees including contractors, consultants and temporary staff engaged by ACC	• Capture decisions or actions recorded in your emails by transferring or recording into the appropriate ACC core system, such as Eos, DocStore or the shared drive. • Report any suspicious emails and/or instant messages to info security team. • Comply with this Policy and any supporting standards. • Comply with all required LIME training modules. • Observe proper email etiquette.
People managers	Must ensure the Email and instant messaging policy is known and followed by staff. Must demonstrate good email and instant messaging behaviours. Must address email and instant messaging issues with the appropriate staff. People managers are responsible for ensuring their staff and contractors are aware of the ACC Email and instant messaging policy This means: • identifying staff, including contractors and fixed-term employees, that require email management training and taking appropriate action to address this • raising email management issues with the Information and Digital Tools team • modelling good practice in Email and Instant Messaging management to their staff.
Information and Digital Tools and Information Security Teams	• Must maintain and administer this policy and associated standards. • Investigate and trouble shoot information security issues and threats. • Reports on and plans for security incidents and threats.

Monitoring and oversight

Information and Digital Tools team with assistance from Information Security will monitor compliance with this policy. Day to day oversight of staff compliance is the role of line managers.

The monitoring and oversight of email and instant messaging follows the five lines of assurance model.

Line of Assurance	Responsibility
1st Line Employees Heads and People Managers	• Ensure email and instant messaging within their business groups is managed per this policy. • Monitors that all team members complete training and learning modules to build information management awareness. • Monitor that their teams are managing email and instant messaging as per this policy. • Monitor tools and technologies which populate reporting dashboards. • Ensure that any incidents are actively raised and addressed with the appropriate employee.
2nd Line Enterprise Data Information and Security (EDIS) team Risk and Compliance Office Chief Technology and Transformation Officer (CTTO)	• Provide oversight of all information management aspects in this policy and subject matter expertise to staff and management when required. • Monitor email and instant messaging usage, and report to the appropriate managers any misuse or suspicious behaviour. • Regularly review and report to ensure the intention of the policy is being honoured. • May conduct periodic compliance review activities on information management practices along with the Privacy team Oerall oversight of our information management practices and through leadership of the Information Governance Group (IGG), and its supporting governance groups, management of all decision making in this.
3rd Line Manager, Service Assurance Assurance Services	• Independently review the overall reliability of processes and performance in accordance with the Assurance Plan. • Provide independent information to the Board and Executive on the reliability of ACC's risk management processes and residual risk status, linked to top value creation and preservation.
4th Line Executive	• CEO and Chiefs have primary responsibility for our strategic objectives and reporting to the Board on the management of these. • Objectives. • Overall responsibility for building and maintaining robust risk management processes.
5th Line Board	• The Board has oversight that ACC is meeting its strategic objectives in relation to information management.

Breaches of policy

Compliance with all policies and procedures is required under ACC's Code of Conduct. Behaviour or actions that are investigated and found to be in breach of the Code of Conduct may result in disciplinary action. Refer to Code of Conduct for further information.

Contacts

Contact Information and Digital Tools IDT@acc.co.nz or Information Security infosec@acc.co.nz.

Definitions

Information Repository	An environment (either electronic or physical) where information is registered, stored and managed.
Record	A record is any documentation or evidence of business activity and decisions.
Business Record	A business record is evidence of a decision or action undertaken as part of conducting ACC business.
Retention and Disposal Authority or Disposal Authority	A systematic listing of the records created by an organisation which plans the life of these records from creation to disposal.

References

InformationmManagement policy

Information security policy

Code of Conduct

Privacy policy

Bullying & harassment policy

Copyright policy

Policy review dates

Last review: December 2018
Next review: December 2020

Appendix A

Overarching documents	
Information Management	• Privacy Act 1993 • Public Records Act 2005 • Official Information Act 1983 • Electronic Transactions Act 2002 • Health Information Privacy Code 2008, revised edition. • Code of Conduct • Information Security Policy • Information Management Policy • Privacy Policy • Health Information Privacy Code 2008 revised edition • ACC Retention & Disposal Schedules

Communication using email Policy v4.0

Summary

Objective
Email is needed in everyday working life and ACC recognises that it is the preferred method of communication for most clients, providers and employers. Our rules for email communication are outlined in this policy, including response timeframes and the types of information we'll accept by email.

Owner [redacted]

Expert Iosef Sengson

Policy

1.0 Agreement to use email as the preferred communication method

a Those who wish to communicate with us via email must:

- agree that email is their preferred method of communication
- provide one preferrred email address contact, ie both work and home email addresses cannot be accepted for clients.
- respond to a verification email to ensure we have the correct version of their email address
- be aware that unverified email addresses cannot be used
- be aware that if a claim has been inactive the email address recorded for the claim must be re-verified.

2.0 Is email the best form of communication?

a Use email for quick and clear communication. Don't use email to vent or try to resolve problems. Information comes across well in email, emotions do not. If you have a problem, pick up the phone and speak directly to the person involved.

NOTE **Example**
You receive an email from a client with a number of questions on the same topic. It's quicker and easier to call the client so you can answer all their questions at once.

3.0 Response timeframes

a We're committed to providing a high standard of customer service at all times. Our clients can expect that we'll answer their emails in a timely manner.

Our customer service standards state that:

- we must respond to all emails within 48 hours

- we encourage clients, providers and employers who communicate with us via email to correspond with a group email address, which is always monitored to ensure we respond within the required timeframe

- if using an individual email account to communicate with clients, providers or employers, staff must ensure that the email address has been verified and all external email correspondence is actioned within these timeframes, regardless of whether or not the staff member is in the office.

4.0 Information we won't accept via email

a We do not accept all information submitted by email. Unacceptable material includes:

- ACC45 injury claim forms (173K). Service Centres will not accept ACC45 injury claim forms from an unsecured network or unverified email address unless there are exceptional circumstances.

- ACC3 employee earnings certificates (221K), or any other earnings details from an unsecured network or unverified email address

- details of a client's earnings where the recipient or sender has not been verified
unsolicited reports

ACC45 ACC Injury claim.pdf

5.0 Information we will accept via email

a • assessments and medical reports

• a client's change of address

• a scanned PDF bank deposit slip, but only if the clients email address has been previously verified

• ACC18 medical certificates from clients

• ACC18 medical certificates from accredited employers or employers who hold an Employer Reimbursement Agreement

• ACC18 medical certificates from a provider using a secure network from their Practice Management System (PMS) or an approved intermediary

• ACC3 earnings certificates from employers using a secure network from ACC Online

• written confirmation of earnings where:

- we can clearly identify that the email has come from that business or verified source

- the signed, faxed or posted version of the ACC3 certificate contains the email address

• we've called the employer, verified we are talking to the correct employer and documented this in Eos 'Contacts'

6.0 Receiving emails from clients, providers and employers

a While we can control the emails we send to people, we don't have the same control over the emails we receive. We trust most providers and employers to be careful about the information they send in their emails. They have duties to their patients or employees and can face disciplinary action from external bodies for breaches of privacy.

• If you receive an attached document that is not a PDF, tell the sender we prefer to receive documents in PDF format, or any other uneditable format, if possible

• If you have any doubt regarding the authenticity of an email, do not open it.

If the email is from...	then...
a client	• when you receive an email, before responding the first thing you need to do is check that it has been sent from a verified email address. See: Verifying client's email using Email Toolset, or Verifying employer contact email using Email Toolset. • you must be satisfied that the information has come from the sender. If in doubt, phone the sender and either confirm they sent the email, or ask them to mail or fax a physical copy. For more information see Risks associated with email communication
a provider	• when you receive an email, before responding the first thing you need to do is check that it has been sent from a verified email address. See: Verifying an existing vendor, provider, or facility work email address.
an employer	• do not act on information contained in the emails unless we've verified the employer and the person sending them • if verified, this will be noted in the Eos 'Contacts' tab

Receiving emails from clients, providers and employers.PNG

7.0 Providers using personal email addresses

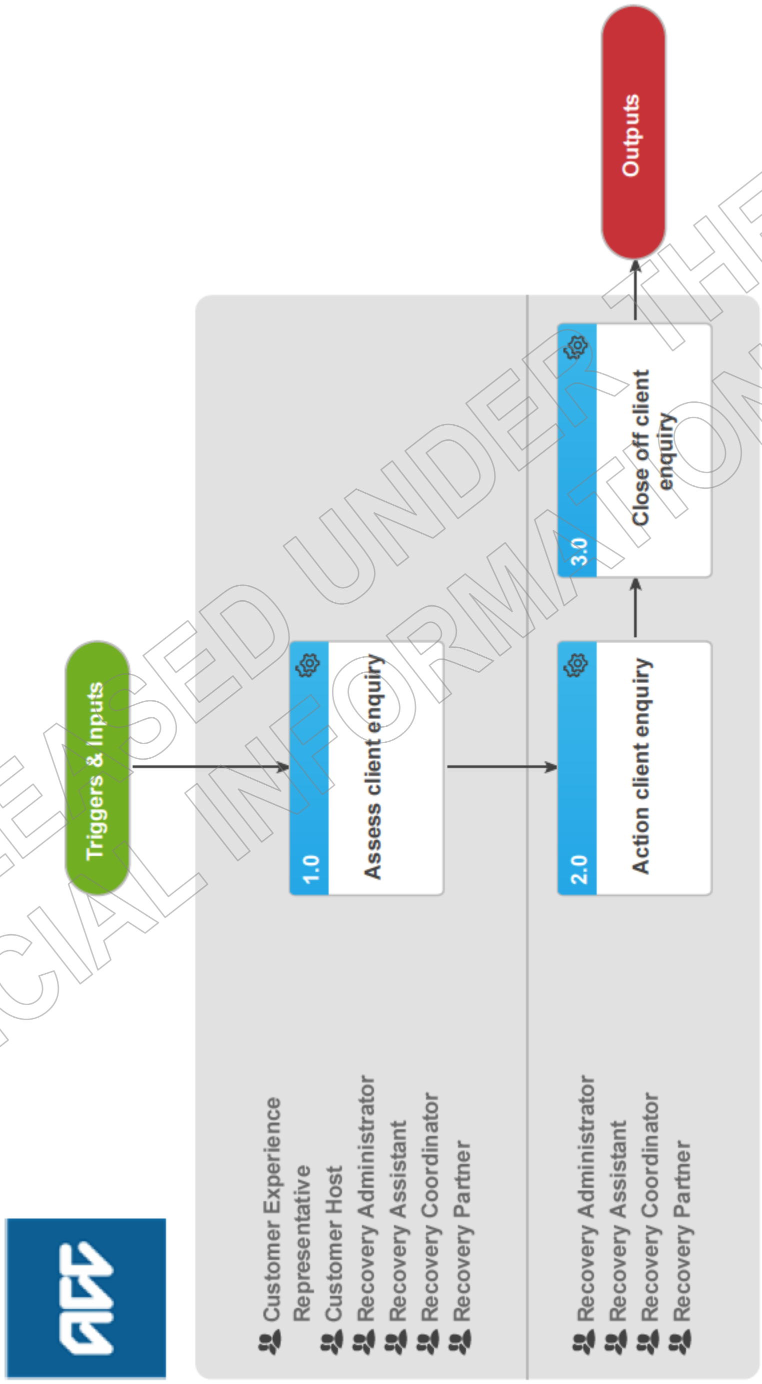
a If a provider chooses to use their personal email address to communicate with us, we consider that address as the official provider email address. This address must be verified before responding to any emails.

Documents and reports that we send to providers are considered to be health information under the Health Information Privacy Code 1994 (the Code). Providers must adhere to the Code and are therefore responsible for the safe and secure storage of any health information we send them.

8.0 Internal emails relating to clients

a Avoid sending internal emails about clients. If you need to send any correspondence about a client and their claim to another internal staff member, use an Eos 'General Task'.

(NGCM) Handle Client Enquiry v11.0



(NGCM) Handle Client Enquiry v11.0

Summary

Objective
The objective of this process is to direct client enquiries to the necessary teams in order for the enquiry to be resolved.

Background
Client enquiries are received through various channels - by phone, email, postal correspondence, in person at an ACC site or customer feedback forms.

Enquiries may be from the client themselves or another party such as the client representative or advocate, or insurer.

This process covers enquiries that are not covered by other processes. Enquiries received by the Client Contact Centre are out of scope because they will follow their own processes and knowledge base through the Vault.

Owner Paul Harvie

Expert Peter Bennett

Procedure

1.0 Assess client enquiry

Customer Experience Representative, Customer Host, Recovery Administrator, Recovery Assistant, Recovery Coordinator, Recovery Partner

a Confirm the type of client enquiry received.

NOTE **What if you receive the client enquiry from another staff member or team?**
Go to 2.0, Action client enquiry.

NOTE **What if the client or their representative phones or emails a Recovery Team Member directly?**
Go to the Identity check Policy to confirm you are dealing with the correct person by asking ACC's identity check questions.

Complete the identity check and go to 2.0, Action client enquiry.

PROCESS Identity Check Policy

NOTE **What if a client or their representative visits a site or hub to speak with someone directly?**
Ask for details about their enquiry. If the enquiry relates to a claim, ask for information such as the claim number or injury date.

Advise a Team Leader there is someone wanting to discuss an issue. The Team Leader can arrange for someone to speak with the client or representative.

While the Team Leader is arranging this, advise the client someone will be with them shortly.

Go to 2.0, Action client enquiry.

NOTE **What if the enquiry is from another party, such as the client's representative, advocate or insurer?**
In Eos, look up the Recovery team member assigned to the client's claim and forward the enquiry to them.

Go to 2.0, Action client enquiry.

NOTE **What if the client or their representative is requesting the client's claim information?**
Go to the Complete Client Information Requests process.

PROCESS (NGCM) Complete Client Information Requests

NOTE **What if the client or their representative wants to update the client's personal details?**
Go to the Update Client Details on Party Record process.

PROCESS (NGCM) Update Client Details on Party Record

NOTE **What if the Contact Centre is able to resolve the query at the first point of contact?**
Add a Contact to the relevant record.

This process ends.

NOTE **What if the client or their representative has a business or levy enquiry?**
Forward the enquiry to business@acc.co.nz and inform the client or their representative that this has been done and that someone will be in contact.

Go to 2.0, Action client enquiry.

NOTE **What if the client or their representative sends a written enquiry via postal services?**
Go to the Upload Physical Documents Received via Postal Services.

PROCESS (NGCM) Upload Physical Documents Received via Postal Services

NOTE **What if the client or their representative sends Heartbeat feedback?**
Follow the Heartbeat Listening to our customers process.

PROCESS Acting on Heartbeat Feedback

NOTE **What if the enquiry could relate to a review application?**
• if the enquiry is an email, forward it to accreviewapplication@acc.co.nz
Reply to the client advising them that the query has been forwarded to the appropriate team and they will be in contact
• if the enquiry is over the phone, advise the client that a review application must be in writing. This can be an email asking for a review and should be sent to accreviewapplication@acc.co.nz.

Go to 2.0, Action client enquiry.

NOTE **What if you need in-house legal advice to help with a client enquiry?**
Email legal.services@acc.co.nz and provide as much background information as you can. For example:
• a description of the issue
• a summary of the key facts
• attach any background information or key documents
• your desired outcome and timeframes.

Go to 2.0, Action client enquiry.

NOTE **What if you need privacy advice to help with a client enquiry?**
Email privacy.officer@acc.co.nz or call them on 46464. You can contact them:
• when you identify, or are advised of, a privacy breach
• if you need advice about any privacy-related matters.

Go to 2.0, Action client enquiry.

NOTE **What if you need assistance from a Clinical Advisor or Technical Specialist to help with a client enquiry?**
Go to the Seek Internal Guidance process.
PROCESS (NGCM) Seek Internal Guidance

NOTE **What if you need assistance from another ACC team to help with a client enquiry?**
Contact the relevant team or speak with your Recovery Leader if you are not sure who to contact.

Go to 2.0, Action client enquiry.

2.0 Action client enquiry

Recovery Administrator, Recovery Assistant, Recovery Coordinator, Recovery Partner

a In Eos, open the client's Claim record.

b Review the enquiry and the client's claim information.

c Respond to the client or their representative with an answer to their enquiry.

NOTE **What if you need to do identity checks?**
Go to the Identity check Policy to confirm you are dealing with the correct person by asking ACC's identity check questions.
PROCESS Identity Check Policy

NOTE **What checks are required before you disclose any information?**
Go to the Privacy check before disclosing information Policy.
PROCESS Privacy check before disclosing information Policy

NOTE **What if you can't answer the enquiry?**
• find out more information, or identify a relevant role and escalate the enquiry, as applicable
• when you are able, respond to the client or their representative with an answer to their enquiry, using the appropriate channel
• if the enquiry may take some time to resolve, let the client know, and keep them informed.

3.0 Close off client enquiry

Recovery Administrator, Recovery Assistant, Recovery Coordinator, Recovery Partner

a Ensure the enquiry has been resolved to the client's satisfaction.

NOTE **What if you have been unable to resolve the enquiry?**
Find out more information, or identify a relevant role and escalate the enquiry, as applicable.

b Close any outstanding tasks or activities when you are satisfied that the enquiry has been resolved.

c In Eos, record a Contact in the client Party record or Claim record and, if applicable, file away the enquiry email.

d Save any email correspondence against the client's claim record or Party record once it has been forwarded to the appropriate team.

NOTE **What is the difference between these records?**
• if the enquiry relates to a specific claim, add a Contact to the client's claim record
• if the enquiry does not relate to a specific claim, or the claim hasn't been received yet, add a Contact to the client's Party claim record.

e Add details of the enquiry, the action taken and any relevant notes.

f Delete any emails from the inbox.