

31 March 2021

[REDACTED]
[REDACTED]

Tēnā koe [REDACTED]

Your Official Information Act request, reference: GOV-009602

Thank you for your email of 7 February 2021 asking for the following information under the Official Information Act 1982 (the Act):

The ACC staff CODE OF CONDUCT and have all information relating to the ACC code of conduct.

Objectives of the code

The ACC staff Code of Conduct (the Code) governs the behaviours of all employees of ACC, to enable us to meet the expectations placed upon us as a Crown Entity. These standards are based on the standards that apply to all State Servants, as detailed in the State Services Standard of Integrity and Conduct.

Attached documentation

Attached is a copy of the Code and the documents referenced at the end of the Code.

- The ACC Code of Conduct
- Bullying and Harassment
- Conflict of Interest
- Protected Disclosure
- Dress code (replaced by Flexible Dress Guide)
- Equal Employment and Opportunity Policy
- Sensitive Expenditure
- Health, Safety and Wellbeing Policy
- Information security
- Internet and Email (included in above policy)
- Media
- Privacy
- Procurement Policy
- Social media (part of Media Policy now)
- Taking Leave Policy

We have not included a copy of the Delegations Manual as this document will soon be available on the ACC website. Refer to <https://www.acc.co.nz/resources/> in Search put in Delegations Manual or Corporate Delegations Manual. This decision has been made under section 18(d) of the Act, the information requested will soon be publicly available.

We have removed some names in these documents, to protect the privacy of individuals. This decision was made under section 9(2)(a) of the Act. In doing so, we have considered the public interest in making the information available and have determined that it does not outweigh the need to protect the privacy of these persons.

Who to Contact

If you have any questions, you can email me at GovernmentServices@acc.co.nz.

If you are not happy with this response, you have the right to make a complaint to the Ombudsman. Information about how to do this is available at www.ombudsman.parliament.nz or by phoning 0800 802 602.

Nāku iti noa, nā

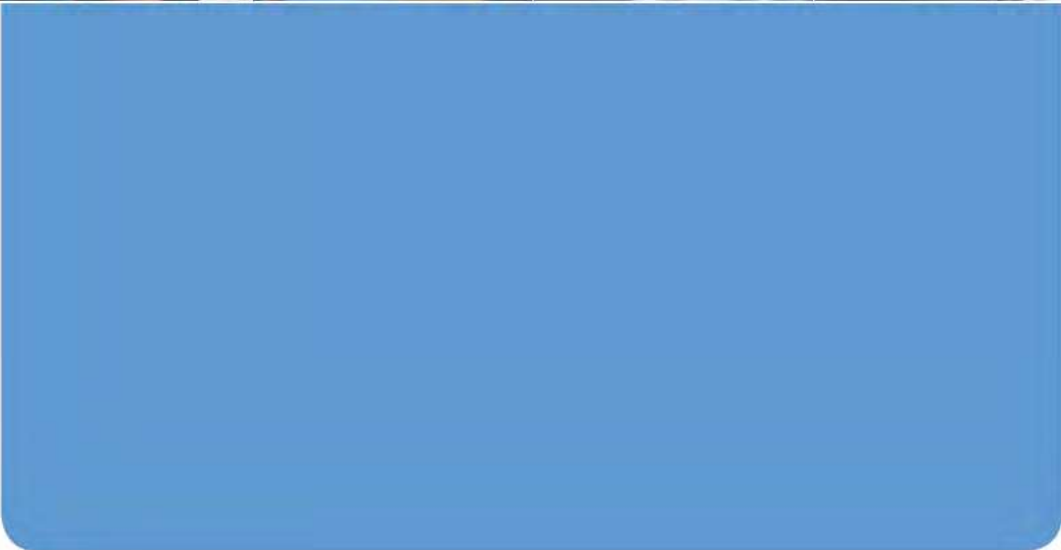
A handwritten signature in black ink, appearing to read 'Sasha Wood', written in a cursive style.

Sasha Wood
Manager Official Information Act Services
Government Engagement & Support



ACC Code of conduct

*The Code of Conduct applies to all
ACC employees and contractors*



1. Code Statement

ACC is charged with the implementation of the Accident Compensation Act 2001. In fulfilling this duty, ACC's vision is to create a unique partnership with every New Zealander, improving their quality of life by minimising the incidence and impact of injury.

As a Crown entity, ACC is part of the State Sector and contributes to building the trust and confidence of citizens in the institutions of government.

All State Sector organisations are expected to work with a spirit of service to the community, to make our services accessible and effective to those who need them, and to strive to make a positive difference to the wellbeing of New Zealanders.

Everyone who works for ACC has an important role to play in making sure we achieve our vision, and in ensuring we maintain our reputation and standing in the perception of the public. Our actions and behaviours must be consistent with these expectations at all times.

2. Objective

This Code governs the behaviours of all employees of ACC, to enable us to meet the expectations placed upon us as a Crown Entity. These standards are based on the standards that apply to all State Servants, detailed in the State Services Standard of Integrity and Conduct.

The Code of Conduct:

- can be used to provide coaching on appropriate conduct
- enables recognition of those who model the desired standard of conduct
- reflects and reinforces the ACC values and behaviour required
- outlines inappropriate behaviour and its consequences.

3. Scope

All ACC employees and contractors are expected to maintain the highest standards of integrity, discretion and ethical conduct when performing duties or representing ACC in any way.

All employees of ACC must read, understand and follow our Code of Conduct.

4. Code standards

You are expected to exercise good judgement to determine what action to take in a given situation.

Your actions need to be able to withstand scrutiny from internal and external parties. Our behaviour and actions must be seen to be fair, impartial, responsible and trustworthy at all times.

In order to achieve the high standards of behaviour expected of us, as an employee or contractor you must:

4.1 Be honest and act with integrity

- In all aspects of your employment (e.g. in your work with clients and levy payers, with regard to work attendance, requests for financial reimbursement, use of sick leave etc).

4.2 Respect the rights of others

- Treat others fairly, courteously, equally, and without discrimination or harassment
- Uphold the rights of clients, as specified in the Code of ACC Claimant's rights
- Respect and respond to all cultures, values and beliefs, particularly Māori and minority groups
- Promote the principles of Equal employment opportunity.

4.3 Perform your duties to the best of your ability

- Prioritise your primary role as an ACC employee over any secondary interests, commitments, values or beliefs you hold personally, and declare any potential Conflict of interest immediately
- Show commitment to a high quality of work
- Adhere to the ACC Health and safety policies in all areas of work
- Comply with all ACC policies, processes and standards
- Model and demonstrate ACC values and behaviours, which underpin decisions about what we do, and how we operate and behave
- Comply with the code of any professional body that you are registered or affiliated with, where this impacts upon your work with ACC
- Show initiative and creativity when resolving problems, seek to maximise productivity, and identify opportunities for improvement
- Make decisions appropriate to your role and be responsible for those decisions and the actions that result from them
- Be supportive of changes made by ACC, as change is necessary for the organisation's success
- Be supportive of your colleagues and accept your responsibilities as a team member
- Manage your personal and workplace relationships appropriately so they do not adversely affect your work.

4.4 Uphold the reputation and standing of ACC

- Act with integrity in any personal dealings you may have with ACC as a client
- Obtain your manager's approval before commencing any activity, business interest or employment that has the potential to conflict with ACC business (e.g. acting as an advocate for a client, undertaking secondary employment)
- Ensure your behaviour in relation to gifts and gratuities, managing contracts and purchasing, and other sensitive expenditure does not compromise (or appear to compromise) your personal integrity or ACC's
- Maintain appropriate professional behaviour when travelling on ACC business
- Maintain appropriate professional behaviour in any situation where you may be perceived as representing ACC
- Have a professional standard of dress
- Engage with the Media team about any media enquiries you receive
- Ensure that your behaviour will not bring ACC into disrepute
- Advise your manager of any convictions or charges laid against you whilst employed by ACC
- Maintain appropriate boundaries and relationships with clients and any other people you may work with.

4.5 Act in a politically neutral manner

- Ensure that your behaviour maintains Ministerial and public confidence in the impartiality of advice given and actions taken
- Ensure that your comments do not bring ACC or the Minister into disrepute, or compromise the perception of ACC as politically neutral (e.g. stating or implying your personal view on an issue as ACC's view)
- Ensure that your personal participation in political matters does not conflict with (or appear to conflict with) your duty to act in a politically neutral manner.

4.6 Use ACC information and property appropriately

- Be responsible for the security and confidentiality of all information that you deal with during your employment with ACC
- Use financial and non-financial information gathered by ACC and your knowledge of ACC's systems and processes only to perform ACC's business
- Treat all ACC assets and property with care and respect
- Take all reasonable steps to protect the privacy of our clients, customers, employees and other stakeholders
- Report any actual or potential privacy breaches to your manager immediately.

4.7 Act within the law

- In particular, the Accident Compensation Act 2001, Official Information Act 1982, Privacy Act 1993, Health Information Privacy Code 1994, Human Rights Act 1993, Employment Relations Act 2000 and any other relevant legislation.

5. Accountabilities

The Chief Talent Officer is responsible for ensuring organisational controls are in place in support of this policy.

6. Responsibilities (including monitoring and oversight)

Role:	Responsibility:
Employees	<ul style="list-style-type: none">• Read, understand and follow this Code of Conduct• Undertake training or confirm your understanding of the Code of Conduct when requested by ACC• Remain up to date with the current Code of Conduct expectations• Discuss any concerns about what may be considered unacceptable behaviour with your manager• Discuss with your manager before you take any course of action that you are not entirely sure falls within the bounds of acceptable behaviour• If you believe someone in ACC is acting unethically, or has been involved in serious wrongdoing, you should report this confidentially through OKtoSay and receive protection under the Protected Disclosure Act.
Contractors	<ul style="list-style-type: none">• Maintain the highest standards of integrity, discretion and ethical conduct when performing duties or representing ACC in any way.

Continued ...

Role:	Responsibility:
Managers	<ul style="list-style-type: none"> • Managers are representatives of ACC both when dealing with external customers or stakeholders, and when dealing with internal employees and contractors • Managers have a lead role in establishing and promoting our expected standards of behaviour and integrity • Managers are expected to conduct their behaviour, actions and decisions consistently with their duty to be fair, impartial, trustworthy and responsible at all times • As a manager you are expected to: <ul style="list-style-type: none"> – Establish and promote ACC’s expected standards of behaviour and integrity – Consider your behaviour, actions and decisions in terms of the expectation to be fair, impartial, trustworthy and responsible at all times – Manage employees in accordance with the Code of Conduct, and any other ACC policies, processes, standards and systems in place to support you as a manager (e.g. development programme, performance management processes) – Lead, model and promote the expected standards of behaviour and integrity within the Code of Conduct and other internal policies and processes – Provide employees with education and coaching on expected standards of behaviour and integrity where needed – Represent ACC positively when interacting with staff, and deliver our policies, changes, initiatives or decisions in a manner consistent with ACC’s intentions – Take ultimate responsibility for work quality, actions and decisions of employees in your team – Manage within your capabilities and take ownership of your own development, and that of your team – Manage within the delegated authorities framework as specified in the Delegations Manual.
Chief Talent Officer	<ul style="list-style-type: none"> • Monitor the effectiveness of the Code of Conduct • Ensure organisational controls are in place in support of this policy.
Executive	<ul style="list-style-type: none"> • Model the highest standard of behaviours according to this Code of Conduct • Ensure Code of Conduct behaviours are integrated into all aspects of ACC business.
Board	<ul style="list-style-type: none"> • Approve the Code of Conduct and ensure it is consistent with ACC’s strategic direction.

7. Monitoring and oversight

Line of Assurance:	Monitoring and oversight:
1st line Employees and Managers	<ul style="list-style-type: none">• Employees are expected to comply with the Code of Conduct.• Managers make employees aware of the Code of Conduct and monitor compliance.
2nd line Talent Group	<ul style="list-style-type: none">• The Talent Group oversees overall compliance with this policy and obtains feedback on its effectiveness.• The Employee Relations Team provides oversight of employment relations issues, including those relating to breaches of the Code of Conduct to ensure that proper procedures are followed.
3rd line Assurance	<ul style="list-style-type: none">• Third line functions provide independent information on the overall effectiveness of the Code of Conduct.• This includes Assurance Services schedule of continuous assurance activities for Talent processes and assessment of our compliance with obligations.
4th line Executive	<ul style="list-style-type: none">• The Chief Executive and Chiefs have overall responsibility for ensuring compliance with Code of Conduct policies and processes.
5th line Board	<ul style="list-style-type: none">• The Board approves the Code of Conduct and ensure it is consistent with ACC's strategic direction.

8. Breaches of Policy

Behaviour or actions that are investigated and found to be in breach of the Code of Conduct may result in disciplinary action. Where breaches are found, ACC's Discipline and dismissal procedures will be followed and the employee will have an opportunity to provide an explanation for their actions or behaviours and have the right to representation.

The action taken will depend on the severity of the breach:

- Breaches of the Code of Conduct that are deemed 'misconduct' may lead to disciplinary action up to and including a final warning
- Breaches of the Code of Conduct that are deemed 'serious misconduct' may lead to disciplinary action up to and including summary dismissal. Summary dismissal is termination of employment without notice or prior warnings.

If any breaches normally considered to be misconduct are very serious or repeated, these may be deemed serious misconduct.

Misconduct

Misconduct occurs when an employee does something wrong (namely, breaches this Code of Conduct or other ACC policy) either by doing something, omitting to do something, or through their behaviour.

The lists below of actions considered to be misconduct or serious misconduct are intended as a guide for employees, and are examples only. They do not constitute an exhaustive list of breaches of the Code of Conduct.

Examples of misconduct include:

- Any act of negligence harming ACC
- Disobeying a lawful and reasonable instruction from a manager
- Failure to meet the standards of performance and behaviour expected of ACC employees
- Inappropriate behaviour or relationships

- Any action which may in any way damage the relationship of trust and confidence between ACC and government, other agencies or the community
- Allowing unauthorised access to, or disclosure of, any matter or information in relation to ACC business
- Misuse of ACC internet and/or email systems
- Inappropriate use of purchasing card or expenses
- Absence from duty or place of work without proper reason or authorisation
- Repeated lateness for work, or repeated absenteeism without just cause
- Failure to comply with any ACC policy or procedure
- Any behaviour of a similar type.

Serious misconduct

Serious misconduct occurs when the misconduct could have the effect of destroying or undermining the relationship of trust and confidence between an employee and employer.

Examples of serious misconduct include:

- Dishonesty
- Theft
- Fraud
- Handling a claim relating to oneself, a relative, acquaintance or friend without the express approval of the manager, or taking a role as an advocate for a client without approval
- Corruption – accepting a bribe, inducement, reward or gift, or complying with a request or threat to use your position to provide a benefit to any person or third party, which has the effect of allowing inappropriate activity or compromising the impartial performance of your duties

- Failure to declare any activity, business interest or employment that has the potential to conflict with ACC business
- Accessing ACC information relating to family, friends, acquaintances or clients without legitimate cause
- Criminal conviction leading to imprisonment or adversely affecting your ability to carry out your work. Offences generally considered unacceptable are outlined in the Screening for Criminal Convictions policy but will be determined according to the nature of the employee's role
- Misuse or unauthorised possession or sharing of ACC property and/or information (e.g. misuse of financial information or client information)
- Harassment of anyone you work with (e.g. client, employee, contractor)
- Abusive or discriminatory statements or practices
- Assaulting or abusing another person
- Allowing work performance to be affected by drug, alcohol or substance abuse (including abuse during work hours)
- Dangerous or unsafe work practices, including non-compliance with ACC Health and safety policies, and Health and Safety legislation
- Any act that has the potential to bring ACC into disrepute
- Significant failure to comply with any ACC policy or procedural requirements
- Any behaviour of a similar type.

9. Contacts

Contact HR Help regarding this policy.

10. References

State Services Standards of integrity and conduct

Policies:

- Bullying and harassment
- Conflict of interest
- Protected disclosure
- Dress code
- Equal employment opportunity
- Sensitive expenditure
- Health and safety
- Information security
- Internet and email
- Media
- Privacy
- Procurement
- Social media
- Taking leave policy
- Delegations Manual

11. Policy review dates

Last review: February 2020

Next review: February 2023

www.acc.co.nz

Bullying and Harassment Policy



POLICY NUMBER	1.1.0
TOPIC	Bullying and Harassment Policy
OWNER	[REDACTED] Head of [REDACTED] Partnership and Organisational Change Executive Leaders Talent
DATE APPROVED	14 September 2018 [REDACTED]
APPROVER	Sharen Champness, Chief Talent Officer
DATE OF REVIEW	14 September 2020

1 Policy Statement

All employees have a right to be treated with dignity and respect at work. As a good employer, ACC will not tolerate workplace bullying or harassment in any form. ACC recognises the destructive impact of such behaviour on individual employees and our organisation as a whole.

2 Objective

This policy sets out ACC's definitions of bullying and harassment and outlines our roles and responsibilities in this area.

Employees are encouraged to report any concerns regarding bullying or harassment occurring in the workplace so these can be addressed appropriately.

3 Scope

This policy applies to all ACC employees and contractors who feel that have been bullied or harassed by another ACC employee or contractor in their role as an employee of ACC.

Out of scope:

1. Bullying or harassment by a client. This will be covered by case management processes.
2. Bullying or harassment by a provider. This will be covered by the provider's contract with ACC.

4 Policy standards

This policy should be read alongside ACC's procedures on [Raising bullying or harassment concerns](#).

4.1 ACC has a legal obligation as a good employer to provide a safe working environment to all employees.

4.2 All employees are entitled to raise a concern about bullying or harassment, even when this behaviour was not directed at them, if they believe this behaviour has affected them.

ACC does not advise raising a bullying or harassment concern on behalf of another employee, as they may not feel comfortable with this approach or could feel undermined.

However, employees are able to report this as serious misconduct confidentially through OktoSay. See [Make a protected disclosure](#) for guidance.

4.3 When a complaint is raised, ACC will consider whether, in those circumstances, a reasonable and objective person would perceive that behaviour or action as bullying or harassment. This will be considered from the perspective of the complainant.

This assessment will be made in line with the definitions provided in this policy.

4.4 Management actions directed at an employee will not be construed as bullying if they are appropriate, and delivered in a reasonable way.

4.5 When determining the most appropriate course of action to address a concern, ACC will consider all relevant information. Considerations include:

- the nature of the concern
- the preferences of the person reporting it
- the availability of evidence supporting the concern
- any known history or context.

For more information on the courses of action that may be taken, see [Raise bullying or harassment concerns](#).

4.6 All parties are entitled to support throughout a bullying or harassment concern by:

- Having a support person or representative.
- Accessing the employee assistance programme.
- Requesting further support from their manager if they require it.

5 Accountabilities

The Chief Talent Officer is responsible for ensuring organisational controls are in place in support of this policy.

6 Responsibilities

Role:	Responsibility:
<p>Employees</p>	<ul style="list-style-type: none"> • In order to keep our organisation free from bullying or harassment behaviours, it is important that we all support our colleagues in preventing these. If you witness someone experiencing bullying or harassment behaviours, encourage them to raise the issue with a manager or Talent. • Make sure you do not engage in behaviour which could be perceived as bullying or harassment. • Report any concerns at an early stage – often when issues are raised early, they can be dealt with more effectively. • Give serious consideration to all of your options in the event of a complaint – both informal and formal. • Be vigilant about bullying or harassment in the workplace and take appropriate steps if a problem is identified • Maintain confidentiality in any investigations you are involved in. • Participate cooperatively in an investigation, if required.
<p>Managers</p>	<ul style="list-style-type: none"> • Make sure you are aware of and understand ACC's bullying and harassment policy. • Make sure you do not engage in behaviour which could be perceived as bullying or harassment • Be vigilant about bullying or harassment in the workplace and take appropriate steps if a problem is identified • Have regular conversations with all employees to ensure there is a forum where issues can be raised at an early stage • Seek advice or assistance from business partners if necessary. • Escalate any issues or queries you are unsure about to Talent to ensure a consistent approach is taken across the organisation • Maintain confidentiality in the event that you are involved in an investigation • Take an appropriate role in managing a formal or informal complaint according to the professional advice received from your Talent Consultant • Participate co-operatively in an investigation, if required.
<p>Senior managers</p>	<ul style="list-style-type: none"> • Take overall ownership for a bullying or harassment complaint in your business group • Take appropriate steps to manage a workplace situation whilst a complaint is being investigated, in consultation with your Talent Consultant • Remain impartial whilst any complaint is being investigated

	<ul style="list-style-type: none"> • Be a consistent point of contact for all affected parties once a complaint has been raised • Make sure any recommendations made as a result of an investigation are implemented effectively in a timely manner.
Talent	<ul style="list-style-type: none"> • Monitor, update and communicate ACC's policy and procedures for managing bullying and harassment, to ensure these remain relevant, appropriate and effective • Provide advice to managers and employees on the application of this policy • Coordinate the resolution of any formal or informal complaint, in accordance with ACC procedures • Manage any allegations of bullying or harassment in a fair, impartial, consistent and effective manner. • Monitor workplace culture at ACC, and analyse information for indications of negative culture that could lead to bullying and harassment. This can be monitored through: <ul style="list-style-type: none"> • Surveys • Exit interviews • Appraisals • Indicators • Inform relevant managers and employees of the outcome of any OktoSay disclosure.
Executive	<ul style="list-style-type: none"> • Exercise due diligence to ensure that ACC meets its health and safety obligations

7 Monitoring and Oversight

Managers will take any necessary steps to address and respond to any bullying and harassment issues at first instance.

Senior managers take overall responsibility for bullying and harassment issues in their business group, and will ensure that bullying and harassment issues are responded to appropriately and consistently, liaising with Talent, managers and interested parties.

Issues will be escalated to Talent if there is any uncertainty.

Talent will:

- Ensure a consistent approach is taken for bullying and harassment issues that are escalated.
- Monitor and update ACC's policy and procedures for managing bullying and harassment issues,
- Monitor overall workplace culture at ACC and analyse information for indicators of a negative culture that could lead to bullying and harassment issues.

8 Breaches of Policy

Complying with all policies and procedures is an expectation outlined in the 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.

Behaviour that breaches the [Harassment Act 1997](#) is a criminal offence, and may result in charges being laid.

9 Contacts

Contact HR Help for any information or assistance regarding this policy.

10 Definitions

Workplace bullying:

“Repeated and unreasonable behaviour directed towards a worker or a group of workers that can lead to physical or psychological harm.

Repeated behaviour is persistent, and may involve a range of actions over time.

Examples of potentially unreasonable behaviours are:

- Belittling remarks.
- Ignoring, excluding or isolating.
- Ridiculing, insulting, or teasing.
- Threats of violence.
- Persistent and/or public criticism.
- Intimidation.
- Reducing opportunities for expression.
- Hints or threats about job security.
- Sabotage.

This list includes examples, and is not exhaustive. Please visit [WorkSafe New Zealand](#) for more information on bullying.

Examples of behaviour that **do not** constitute bullying/unreasonable behaviour include:

- One-off or occasional instances of forgetfulness, rudeness or tactlessness
- Setting high performance standards because of quality, safety or customer service
- Constructive feedback and legitimate advice or peer review
- A manager requiring reasonable verbal or written work instructions to be carried out
- Legitimate management of leave, performance, misconduct or other workplace concerns under ACC's respective policies and procedures
- A single incident of unreasonable behaviour (but it could escalate and should not be ignored. It would be sensible to address this when it occurs)

Harassment:

An act that breaches the [Harassment Act 1997](#). For example:

- [General harassment](#) could include any unwanted or unjustified behaviour which another person finds offensive or humiliating, and because it is serious **or** repeated, has a negative effect on the person's employment, job performance, or job satisfaction. This may include:
 - Comments or behaviour that express hostility, contempt or ridicule, repeated put downs for people of a particular age, body shape, gender identity etc
 - A general work atmosphere of repeated jokes, teasing, or 'fun' at someone else's expense because of a particular characteristic they have
- [Racial harassment](#), as defined in the Employment Relations Act 2000
- [Sexual harassment, as defined in the Employment Relations Act 2000](#).

Interpersonal conflict and performance management are common occurrences within the workplace. They are both normal and legitimate within any organisation, so long as they are managed in line with any relevant procedures (e.g. the performance development cycle, coaching processes, or the performance improvement process for performance management) and through professional and respectful behaviours.

Interpersonal conflict and performance management can sometimes be confused with workplace bullying or harassment. They can be challenging to deal with for any employee. If you have a concern about behaviour or actions relating to interpersonal conflict or performance management you should raise this with your manager, their manager, or the person you re in conflict with if you feel able to do so.

11 References

[Employment Relations Act 2000](#)

[Human Rights Act 1993](#)

[Harassment Act 1997](#)

[Solving employment relationship problems at ACC](#)

[Employee Assistance Programme](#)

[Health and Safety](#)

[Equal Employment Opportunity](#)

[Code of conduct](#)



Conflict of Interest Policy

POLICY NUMBER 1.2.0

TOPIC ██████████ Conflict of Interest Policy

OWNER ██████████ Chairperson
Chief Talent Officer
Talent

DATE APPROVED 20 February 2020
██████████

APPROVER Chief Talent Officer

DATE OF REVIEW February 2023

1 Objective

The Conflict of Interest Policy aims to ensure that any conflicts of interest that arise are identified, disclosed and resolved or managed in a timely and effective manner.

2 Scope

This policy applies to all ACC employees and contractors.

3 Policy Statement

As part of the State Sector, ACC is expected to work with a spirit of service to the community. This relies on the public having trust and confidence in ACC. To maintain this relationship with the public, all employees and contractors are expected to maintain high standards of integrity, discretion, and ethical conduct. This includes impartiality and political neutrality. Conflicts of interest may create risk to ACC's finances or reputation. In order to respond to these expectations and risks, conflicts of interest must be transparently declared and effectively managed.

The conflict of interest policy provides a set of principles and processes for resolving and/or managing actual, potential or perceived conflicts of interest.

3.1 It is expected that an employee's role at ACC takes precedence over any secondary interests, commitments, or associations an employee may personally hold.

3.2 Employees must ensure that their outside interests or associations do not adversely affect their work commitment to ACC or conflict with ACC's interests.

3.3 Employees must not state or imply that their personal view on a matter is representative of ACC's position or view.

Where employees share their opinions within the public domain, they should consider whether a conflict of interest could be perceived to arise between their position as an ACC employee and the opinion that they have expressed.

3.4 Any existing employment activity, interest or association that could in any way conflict with ACC business must be declared prior to employment with ACC. In addition, any employment activity, interest or association that arises in the course of employment, and could in any way conflict with ACC business must be approved prior to it commencing.

This includes, but is not limited to, anything that may:

- Conflict with an employee's ACC duties (e.g. working in a medical centre that provides services to ACC clients)
- Compromise an employee's ACC duties (e.g. working as an advisor to a claimant advocacy group or taking a role as an advocate for a client)
- Impact an employee's financial position
- Impair performance (e.g. working at a second job or as a volunteer that may result in being too tired to undertake the normal duties of their ACC role)
- Compromise an employee's integrity (e.g. being in a management position over a partner/spouse or relative)
- Compromise an employee's political neutrality (e.g. standing for election, or an association with a Member of Parliament).

3.5 Employees involved with the procurement of goods and services must be familiar with the Office of the Auditor General guidelines for managing conflicts of interest ([external link](#)) and the Procurement policy.

4 Accountabilities

The Chief Talent Officer is responsible for ensuring organisational controls are in place in support of this policy.

5 Responsibilities

Role:	Responsibility:
-------	-----------------

<p>Employees</p>	<ul style="list-style-type: none"> Employees are responsible for identifying, declaring and addressing any actual, perceived or potential conflict of interest they may have. ACC4818 Declaration of interests and associations (61KB) <p>Employees should ensure they:</p> <ul style="list-style-type: none"> inform their manager of any actual, perceived or potential conflicts of interest formally declare them inform their manager and the Talent team if a declared conflict is no longer relevant ensure they advise their new manager of any existing declared interests (and new interests) when they transfer to a new role or team in ACC. <ul style="list-style-type: none"> If an employee is in any doubt they should seek advice from their manager or Talent.
<p>Managers</p>	<ul style="list-style-type: none"> Discuss potential conflicts with employees and if a conflict exists, agree on ways in which the conflict may be resolved and/or managed. This includes a discussion when a new employee joins the team. Conflicts of interest may be resolved or managed in one of the following ways: <ul style="list-style-type: none"> Declining permission for an employee to undertake a secondary interest. Reaching an agreement with any secondary employer, that the employee has no involvement with ACC clients in their secondary role. Implementing controls to manage a potential conflict of interest eg alternative reporting arrangements. A period of leave or absence is agreed to allow the employee to participate in any activity that is a perceived conflict of interest until the activity is concluded. If it is not possible to resolve/manage the conflict of interest and it renders the employee unable to carry out their role, the employee may be redeployed to a role where the conflict of interest does not exist. If the conflict cannot be resolved and/or managed in any of the above ways, the employee may be dismissed, as a last resort. <p>Report conflicts of interest you are made aware of to Talent on a monthly basis.</p> <p>Advise the relevant Chief of any high risk conflicts as soon as practicable.</p> <ul style="list-style-type: none"> If an employee informs you that an existing conflict is no longer relevant, ensure the Talent team is formally informed of this.

Released under the Official Information Act 1982

Talent	<ul style="list-style-type: none"> • Maintain a register of conflicts of interest and send it to Procurement (including conflicts declared during recruitment and throughout employment) • Monitor employment associated conflicts of interest and refer other conflicts of interest to the relevant business unit.
Procurement	<ul style="list-style-type: none"> • Monitor conflicts of interest relating to Procurement activities on a regular basis.

6 Monitoring and oversight

Role:	Responsibility:
Employees and Managers (1 st line)	<ul style="list-style-type: none"> • Employees are expected to comply with this policy. • Managers will ensure employees are aware of and comply with this policy.
Talent and Procurement (2 nd line)	<ul style="list-style-type: none"> • The Talent Group will monitor overall compliance with this policy and obtain feedback on its effectiveness. • The Procurement team will monitor compliance with this policy within procurement activities.
Assurance (3 rd line)	<ul style="list-style-type: none"> • The Assurance team will audit policies and procedures and arrange for independent auditors when required
Executive (4 th line)	<ul style="list-style-type: none"> • The Chief Executive and Chiefs have overall responsibility for ensuring compliance with conflict of interest policies and processes.
Board (5 th line)	<ul style="list-style-type: none"> • The Board have oversight for ensuring conflict of interest risk is managed well.

7 Breaches of Policy

Complying with all policies and procedures is an expectation outlined in the 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 the Code of Conduct for further information.

8 Contacts

Contact HRHelp for information or assistance regarding this policy.

9 Definitions

A conflict of interest occurs when an employee has a personal interest or duty that may affect their responsibilities at ACC. For example, that personal interest or duty could be:

- A position they hold outside of ACC
- An activity they undertake outside of ACC
- Associations, such as family relationships or other close relationships

An employee's responsibilities at ACC may be affected if, because of that interest: they cannot effectively perform their role; they are perceived as being unable to effectively perform their role; or there is the potential that they may be unable to effectively perform their role.

10 References

Sensitive Expenditure
Procurement
Code of Conduct
[Crown Entities Act](#) 2004

Released under the Official Information Act 1982

Protected Disclosure Policy



POLICY NUMBER	1.3.0
TOPIC	Protected Disclosure Policy (Level two policy)
OWNER	██████████ ██████████ Manager, Integrity Risk Advisory Integrity Services Risk and Assurance
DATE APPROVED	17 August 2022
APPROVER	Herwig Raubal Chief Risk and Actuarial Group
DATE OF REVIEW	17 August 2022

1 Objective

This policy aims to increase ACC's integrity maturity by:

- Encouraging our people to raise concerns about any wrongdoing at work, without fear of punishment or reprisal
- Guide our people to disclose concerns using one of the disclosure channels on the [OK2Say page](#) (e.g. speaking to their manager, using OK2Say etc.)
- Protecting our people who disclose information (including a protected disclosure under the [Protected Disclosure Act 2000](#) about serious wrongdoing).

2 Scope

This policy applies to all ACC staff (permanent, temporary, casual employees, contractors and consultants) working on behalf of ACC.

3 Policy statements

Our people raising concerns of wrongdoing (serious or otherwise) will be protected without fear of reprisal or punishment.

Serious wrongdoing is defined (Protected Disclosures Act 2000, section three) as an:

- unlawful, corrupt, or irregular use of funds or resources of a public sector organisation
- act, omission, or course of conduct that constitutes a serious risk to public health or public safety or the environment

- act, omission, or course of conduct that constitutes a serious risk to the maintenance of law, including prevention, investigation, detection of offences and the right to a fair trial
- act, omission, or course of conduct that constitutes an offence
- act, omission, or course of conduct by a public official that is oppressive, improperly discriminatory, or grossly negligent, or that constitutes gross mismanagement.

Examples of serious wrongdoing are:

- committing a crime or offence or covering up a crime or offence
- using public funds for private expenses
- assaulting ACC employees, clients or providers
- engaging in conduct that poses a serious risk to the safety of others
- selling client information
- unlawfully destroying official documents.

Our people will feel safe raising concerns about anything they see, or a situation or work behaviour, that doesn't feel right.

ACC is charged with the implementation of the Accident Compensation Act 2001. In fulfilling this duty, ACC's values include being responsible stewards of our resources and to be fair and transparent in our dealings.

As part of the State Sector, ACC contributes to building the trust and confidence of citizens in the institutions of government. New Zealand is held in high regard for the standards of honesty, openness, transparency and integrity of its State Services. ACC's reputation depends on our ability to build and maintain a culture that promotes speaking up about wrongdoing. Good policies and processes that encourage staff to speak up about possible wrongdoing are vital for maintaining the integrity of our State Services.

Te Kawa Mataaho - the Public Services Commission - (previously the State Services Commission) expect public servants must be able to raise concerns without fear of punishment or reprisal. Everyone who works for ACC has an important role to play in making sure we live our values ensuring we maintain our reputation and standing in the perception of the public.

[Ok2Say](#) provides a safe mechanism for all ACC staff to speak up through a variety of channels about possible wrongdoing in ACC without fear of reprisal. ACC does not tolerate any form of retaliation against anyone (either internally or externally) who speaks up in good faith.

Protections conferred by the [Protected Disclosure Act 2000](#), do not apply where an allegation is made knowing it to be false or made in bad faith.

All issues raised are treated in confidence and ACC will maintain your confidentiality so far as reasonably possible.

4 Policy principles and standards

Reporting information is key to identifying and managing wrongdoing.

The [Protected Disclosures Act 2000](#) sets out the minimum requirements for organisations to meet.

These include operating, publishing and regularly updating internal procedures for receiving and dealing with reports of serious wrongdoing.

Te Kawa Mataaho - the Public Services Commission standards [Speaking up in the State services](#) outline additional expectations on ACC to support effective reporting and managing of wrongdoing concerns.

ACC values, [Code of Conduct](#) and internal processes are designed to ensure that we meet the expectations of Te Kawa Mataaho, the Public Services Commission.

The [Speaking up in the State Services](#) highlights three key elements to encourage a culture of speaking up when any wrongdoing is suspected:

1. Organisational commitment to leadership and culture
2. Robust processes
3. Keeping people safe

How each of these elements work at ACC is explained below.

4.1 Organisational commitment to leadership and culture

ACC will:

- *treat the details of any inquiry into suspected serious wrongdoing in confidence.* Only people involved in the assessment and inquiry of suspected wrongdoing will know the details of the allegation.
- *contact the discloser as soon as possible if confidentiality cannot be maintained* (e.g. the information is vital for proving or disproving the allegation or required for the principles of natural justice).

4.2 Robust processes

ACC will:

- *maintain and promote procedures* for receiving, assessing and managing disclosures of serious wrongdoing
- *have a primary point of contact for disclosures* of serious wrongdoing responsible for assessing any risk of reprisal, repercussion or adverse impact to anyone
- *maintain a Disclosure Committee* which regularly meet to consider and action disclosures raised
- *ensure inquiries are evidence-based* and the person who raised serious wrongdoing will be informed on progress.

4.3 Keep people safe

ACC will:

- *protect our people who disclose information* in good faith about a suspected serious wrongdoing
- *ensure our people do not experience any form of retaliation* as a result of highlighting possible integrity breaches
- *treat disclosure as confidential* and we'll not disclose your name without talking to you first. See [Ok2Say](#) - refer "Being fair" section for examples
- *help and support our people* through the process once an allegation has been received.

5 Accountabilities

The Chief Risk and Actuarial Officer is accountable, through the Head of Integrity Services, for ensuring that this policy is implemented. This includes ensuring accurate supporting operational guidelines, advice, monitoring and reporting are in place and readily accessible for staff.

6 Responsibilities

The expectation of New Zealanders that ACC be a responsible steward, ensuring the appropriate and lawful use of public funds and resources at all times, and ACC's behaviour standard "I am accountable" underpins the responsibility of our people at all levels.

Our people are expected to maintain the highest standards of integrity, discretion and ethical conduct when performing duties or representing ACC in any way.

Role	Responsibility
Employees / Contractors	<ul style="list-style-type: none"> • Discuss any concerns of suspected serious wrongdoing with your manager or report this confidentially through Ok2Say and receive protection under the Protected Disclosure Act <p>If you believe someone in ACC is acting unethically, or has been involved in any wrongdoing, you should report this confidentially through Ok2Say and receive the same protection offered under the Protected Disclosure Act. For more information, visit Ok2Say.</p>
Managers	<ul style="list-style-type: none"> • Lead role in establishing and promoting our expected standards of behaviour and integrity • Conduct their behaviour, actions and decisions consistently with their duty to be fair, impartial, trustworthy and responsible at all times.
Head of Integrity Services	<ul style="list-style-type: none"> • Ensure organisational controls are in place in support of this policy • Overall responsibility and accountability for the implementation of this policy.
General Counsel	<ul style="list-style-type: none"> • Act as the Company Disclosures Officer and Chair of the Disclosure Committee • Point of contact for disclosures of serious wrongdoing • Handle the collection of information and coordination of enquiries with the Disclosure Committee.

Disclosures Committee	<ul style="list-style-type: none"> • Undertake annual reviews of the effectiveness of the protected disclosure policy, associated policies and procedures • Ensure compliance with the Protected Disclosures Act 2000 (link to external website) • Ensure all reported instances of suspected wrongdoing and serious wrongdoing are triaged and an appropriate course of action agreed upon • Observe trends and provide insights to the Chief Executive.
Executive and Board	<ul style="list-style-type: none"> • Model the highest standard of behaviours according to ACC Code of Conduct • Ensure Code of Conduct behaviours are integrated into all aspects of ACC business.

7 Monitoring and oversight

Lines of Assurance:	Role	Monitoring & Oversight
1st Line	Employees and People Managers	<ul style="list-style-type: none"> • All employees remain alert to potential breaches of the Policy and report potential and actual breaches to their manager • All people managers ensure that (i) breaches brought to their attention are documented¹, (ii) notification of the breach is provided to the owner of the Policy within five days of the breach occurring
	Group Risk and Compliance Manager and/or Advisor (if applicable)	<ul style="list-style-type: none"> • Supports employees to determine whether events constitute actual breaches of the Policy • Escalates breaches to the Group's Leadership Team and Chief when appropriate • Stakeholder reporting includes identification of systemic issues (and recommendations on how these are addressed) that may undermine public confidence in the Scheme and ACC • Updates risk registers as required.
	Policy Owner	<ul style="list-style-type: none"> • The Policy Owner ensures that the Group (and other parts of ACC if applicable) responds appropriately to Policy breaches and requests for exceptions.

¹ The "Policy Breach Template" can be used for this purpose but is not mandatory.

Lines of Assurance:	Role	Monitoring & Oversight
2nd Line	Enterprise Risk Team	<p>Performs periodic oversight activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches</p> <p>Reports to the Executive and the Board on the outcomes of such activities.</p>
	Integrity Services	<p>Integrity Services is the lead business group for ensuring adherence to the policy.</p> <p>Integrity Services monitor and evaluate reported instances emerging threats to minimise the likelihood and impact of integrity risk from occurring.</p>
3rd Line	Internal Audit (and external providers)	<p>Performs periodic audit activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches</p> <p>Reports to the Executive and the Board on the outcomes of such activities.</p>
4th Line	Executive	<p>Ensures each Group has sufficient emphasis on risk management and meeting compliance obligations</p> <p>Ensures effective processes and monitoring are in place to meet compliance obligations for the Policy</p> <p>Acts in an appropriate and timely manner in response to reports received that alert the Executive to opportunities to improve Policy compliance activities</p>
5th Line	Board	<p>Responsible for approving any material changes to the level 1 Policies, including text related to monitoring and oversight of compliance with the Policy</p> <p>Acts in an appropriate and timely manner in response to reports received that alert the Board to opportunities to improve Policy compliance activities.</p>

8 Breaches of Policy

The Code of Conduct requires compliance with all ACC policies and procedures. Behaviours 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.

9 Contacts

The [Manager Integrity Risk Advisory](#) is the point of contact regarding issues of interpretation or management of this policy.

10 References

[Speaking up in the State Services | Te Kawa Mataaho the Public Services Commission](#)

Version Control - This should reflect the review process.

Version	Date	Change reason	Who
1.0	10/06/2020	Initial policy reviewed and updated to new template	Risk and Assurance Advisor
2.0	08/09/2020	New policy agreed and signed off by Chief Risk and Financial	Chief Risk and Actuarial Officer

Released under the Official Information Act

Flexible dress guide

We want you to feel comfortable at work and able to 'dress for your day'. We trust you to make the right decision about what you wear, depending on what you've got happening.

Contact [HR Help](#)

Last review 31 Jul 2020

Next review 26 Jan 2021

Here are some things to think about when you're dressing for your day:

- If you have a formal meeting, important meeting, or are welcoming a significant visitor, then your dress might be more formal than your every day wear. You could consider formal cultural dress, dress trousers and a shirt/top, or perhaps a dress or skirt and top and maybe a smart jacket, all teamed with clean footwear. If you're meeting someone you think might feel intimidated or uncomfortable with you dressing more formally, then we trust you to make the right choice
- If you don't have any important meetings, visitors, or clients who would find formal dress more appropriate, then wearing smart casual is your call. For example, dress shorts, tidy jeans or trousers, tidy tops, shirts, or tee shirts.
- Whether it's formal or smart casual, we also welcome cultural dress at any time
- If you're in any doubt, keep your beach wear, nightclub outfit, and gym wear for your weekends and holidays. It's all about showing respect for the situation and people around you. So if it has explicit or offensive content, then work is probably not the right time or place to wear it

Example of formal wear - when you have important people to see or someone important is visiting



Example of formal wear - when you're seeing the minister or someone significant



Example of smart casual - no meetings today



Cultural attire welcome - for example



These guidelines are effective as of 25 July 2019

Released under the Official Information Act

Equal Employment Opportunity Policy



POLICY NUMBER	2.2.0
TOPIC	Equal Employment Opportunity Policy
OWNER	[REDACTED] Head of [REDACTED] Delivery Talent [REDACTED]
DATE APPROVED	19/2/2020
APPROVER	Chief [REDACTED]
DATE OF REVIEW	February 2023

1 Objective

The Equal Employment Opportunity policy aims to ensure alignment of ACC's activities with EEO principles and practices, enabling equity and diversity across the organisation.

2 Scope

This policy applies to all ACC employees, including contractors and any other persons acting for our organisation.

3 Policy Statement

We are committed to being an Equal Employment Opportunity (EEO) employer through organisation-wide [EEO good employer practices](#) relating to the recruitment and selection, development, management and retention of our people.

EEO principles ensure that all job-seekers and employees are considered for the employment of their choice, and that they have the chance to perform to their full potential. The aim of the EEO policy is to:

- Create a versatile workplace that enables productive and effective work
- Ensure ACC selects the best-suited person or team for the job
- Remove barriers to success, so all employees have a chance to perform to their best
- Maximise the potential of New Zealand's diverse population
- Value and respect individuals and their abilities, backgrounds and talent.

3.1 Appointments will be merit-based, considering knowledge, skills, abilities, experience, personal qualities and formal qualifications.

ACC values the diverse talents of our employees and will continuously strive towards excellence in providing equal employment opportunities. ACC employs from a wide cross-section of talent, and selections are made in an open and non-discriminatory manner.

3.2 We identify barriers and take proactive steps to ensure everyone is treated fairly and equitably, and has the opportunity to perform at their full potential

All employees receive equitable opportunities for development, irrespective of gender, race, marital status, age, disability, sexual orientation, religious or ethical beliefs. Opportunities for development will be determined based on organisational, team and individual development needs

3.3 We will not tolerate discrimination or harassment in any form.

All employees have the right to be treated with dignity and respect at all times.

3.4 We will observe the principles of the Treaty of Waitangi

- Partnership
- Participation
- Protection

4 Accountabilities

The Chief Talent Officer has accountability for operational implementation of this policy.

5 Responsibilities

Role:	Responsibility:
Employees	<ul style="list-style-type: none">• Adhere to all EEO principles and practices
Managers	<ul style="list-style-type: none">• Adhere to all EEO principles and practices• Treat employees fairly and equitably in all aspects of their employment• Create and maintain a team environment that observes EEO practices and principles.• Investigate employees' EEO complaints

<p>Talent Group</p>	<ul style="list-style-type: none"> • Monitor the impartial selection of qualified personnel • Oversee the following practices to comply with the principle of being a good employer to ensure fair and proper treatment of our employees in all aspects of their employment: <ul style="list-style-type: none"> ○ Health and Safety Programme ○ EEO Programme ○ Recognition of the aims and employment needs of Maori ○ Recognition of the aims and cultural differences of ethnic and minority groups ○ Recognition of the employment needs of women ○ Recognition of the employment needs of people with disabilities. • Monitor and take appropriate action for any EEO complaints.
<p>Assurance Services</p>	<ul style="list-style-type: none"> • Review the results of monitoring activities, provide an independent assessment, and report on compliance with this policy as required.

6 Monitoring and oversight

Lines of Assurance:	Monitoring & Oversight
<p>Employees and Managers (1st line)</p>	<p>Employees are expected to comply with this policy.</p> <p>Managers will ensure employees are aware of and comply with this policy. Managers will deal with issues of non-compliance within their areas of responsibility.</p>
<p>Talent (2nd line)</p>	<ul style="list-style-type: none"> • The Talent Group will monitor overall compliance with this policy and will take appropriate action for any EEO complaints.
<p>Assurance (3rd line)</p>	<p>The Assurance team will audit policies and procedures and arrange for independent auditors when required</p>
<p>Executive (4th line)</p>	<p>The Chief Executive and Chiefs have overall responsibility for ensuring compliance with EEO policy.</p>
<p>Board (5th line)</p>	<p>The Board have oversight for ensuring EEO risk is managed well.</p>

7 Breaches of Policy

Complying with all policies and procedures is an expectation outlined in the 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.

Sensitive Expenditure Policy



POLICY NUMBER	4.3.0
TOPIC	Sensitive Expenditure Policy which is a subordinate policy to the Finance policy
OWNER	Manager, Business Improvement and Support Procurement Services Finance and Performance Group
DATE APPROVED	10 October 2018 – to be effective from 1 November 2018
APPROVER	John Healy Chief Finance Officer
DATE OF REVIEW	10 October 2020

1 Policy Statement

The Sensitive Expenditure policy provides a set of principles and rules for managing expenditure which by its nature creates financial and reputational risk for ACC. This policy follows the guidance provided by the Office of the Auditor General on controlling sensitive expenditure for public entities except for loyalty benefits. Sensitive expenditure is expenditure by a public entity that could be seen as giving some private benefit to an individual employee that is additional to the business benefit.

2 Objective

As a Crown Entity, ACC has stewardship responsibility for managing money derived from levy payers and general taxation. This means that ACC is subject to the standards of probity and financial prudence which are expected of a Crown Entity, and should ensure that all expenditure is able to withstand public and parliamentary scrutiny.

The purpose of this policy is to establish a framework that will ensure a consistent approach to sensitive expenditure in accordance with ACC's business objectives and which will protect employees and ACC from possible criticism about sensitive expenditure.

The objective of this policy is to ensure that:

- Sensitive expenditure is incurred primarily for business purposes, and that any private benefit to individuals is incidental
- Decisions in approving/incurring such expenditure are made in a sound and defensible manner
- A culture of probity is encouraged within ACC

3 Scope

Sensitive expenditure is defined as expenditure that provides, has the potential to provide, or has the perceived potential to provide a private benefit to employees of a public entity that is additional to the business benefit. It also includes expenditure by a public entity that could be considered unusual for the entity's purpose and/or functions.

This policy gives our employees and contractors a framework in which to operate. It also applies to travel and accommodation for consultants.

The following are potential areas of sensitive expenditure covered by this policy:

1. Travel and accommodation
 - Air travel
 - Accommodation
 - Road travel
 - Food and drink while travelling
 - Expenses
2. Entertainment and hospitality
 - Food and drink
3. Employee benefits and use of assets
 - Koru Membership
 - Loyalty reward scheme benefits
 - Professional memberships
 - Sale of surplus assets to Employees
 - Private use of ACC's assets
 - Private use of ACC's suppliers
4. Employee support and welfare expenditure
 - Clothing/Corporate wardrobe
 - Long service recognition
 - Farewells and retirements
 - Life events
 - Employee recognition
 - Employee/event sponsorship
5. Contributions and gifts to external parties
 - Donations
 - Koha/Meaalofa
 - Gifts to external parties
 - Gifts and Gratuities

The policy also covers the way in which we pay and reimburse for sensitive expenditure

1. Payment by purchasing card
2. Payment by invoice
3. Payment by cash reimbursement

4 Policy standards

Sensitive expenditure receives more scrutiny than other costs. ACC expects those who request and approve sensitive expenditure to understand ACC's policy and guidance on sensitive expenditure.

ACC expenditure should be:

- consistent with the standards of probity and financial prudence that are expected from a Crown Entity; and
- able to withstand parliamentary and public scrutiny.

This policy adopts a principles based approach to sensitive expenditure. The principles are designed to give a balanced approach to individual circumstances.

The principles are that expenditure decisions:

- have a justifiable business purpose
- preserve impartiality
- are made with integrity
- are moderate and conservative, having regard to the circumstances
- are transparent
- are appropriate

4.1 Travel and accommodation

Our travellers, travel arrangers and approvers are expected to:

- Firstly consider if teleconference and video conference calls would produce the same result in a more timely and cost effective manner than travel.
- Make the traveller's safety paramount
- Plan travel that requires the least time away from the office
- Use the most cost effective method of travel taking into account the number travelling
- Take the most direct route to the destination
- Arrange meetings to take into account the travel logistics of participants rather than arranging travel around meetings
- Book as far in advance of travel as practical – at least one week in advance
- Use ACC's preferred suppliers.

Air Travel

- Personal, spouse and companion travel may be combined with business travel if at no additional cost to ACC.
- Any work time used for private travel must be booked as annual leave before the employee leaves
- If an employee is required to change personal travel arrangements for business purposes, ACC will meet any reasonable costs on a case by case basis. Chief Officer approval is required.
- All Air Travel will be economy unless the flight is more than 9 hours long where approval may be obtained by the Chief Executive for a higher class.

Accommodation

- ACC's preferred accommodation providers must be used and within cap where possible. Where there is no preferred accommodation available, other suppliers may be used.
- Individuals may claim for a private accommodation allowance in lieu of staying at a preferred provider. Prior approval from the line manager is required.

Road Travel

- The most cost effective method of travel will depend on the circumstances. This may be rental, fleet car, taxi or public transport. Private car can be used when no fleet vehicle is available or the situation is not suitable such as traveling to the airport. Prior approval must be obtained from the line manager and should be noted on the cash imbursement.

Food and Drink while travelling

- The cost of meals and drinks must be within the Catering and Meals guidelines
- ACC does not pay for mini-bar or alcohol expenses.

Expenses while travelling

- Cash advances, in exceptional circumstances, may be provided when travelling overseas, with approval of the Chief Financial Officer.
- ACC will pay actual and reasonable expenses while travelling on business
- Ensure costs are within the prescribed daily Catering and Meal limits
- We must use the most cost effective method of communication.
- ACC does not cover the costs of tipping by employees while travelling for business purposes in New Zealand.
- ACC will cover the costs of tipping by employees when travelling internationally for business, although tips shouldn't be extravagant and should only occur where tipping is local practice.

4.2 Entertainment and hospitality expenditure

Entertainment is defined as business expense when:

- building relationships;
- representing the organisation at an event or similar;
- when recognising a significant business achievement; or
- celebrating events such as Christmas and retirement functions

Hospitality can cover a range of expenditure from tea, coffee, and biscuits served at meetings to catered events.

Provision of [Food and Drink](#) is acceptable for:

- [Farewell functions](#)
- Employee celebrations
- Meetings or Workshops
- Business networking

ACC will contribute towards employee Christmas parties at an amount set by the Chief Executive each year. This contribution may not be used for the purchase of alcohol.

When entertaining external guests, the meal limits should act as a guide and should be actual and reasonable.

All alcohol must have prior approval of the relevant Chief Officer.

Our [Food and Drink](#) pages give you all the information you need on how to incur and account for this expenditure.

4.3 Employee benefits and use of assets

Loyalty reward scheme benefits

Loyalty reward schemes tend to be given to the named individual who orders or purchases the goods or services, regardless of who has paid for them. Examples include Airpoints and Flybuys. Employees are able to use loyalty rewards for their personal benefit.

Koru Membership

ACC may provide Air New Zealand Koru Club Membership for employees who fly a [significant amount](#)

Professional memberships/ subscriptions

Professional memberships to associations and subscriptions (paper or electronic) may be paid on behalf of an employee by ACC when it is required for professional registration purposes, is relevant to the performance of the employee or as part of their contract. If not within contract, ACC will pay for one membership provided it is clearly relevant to the performance of the employee's current duties and responsibilities.

Sale of assets to employees

The Chief Financial Officer may determine if any redundant fixed assets can be sold to employees. Refer to [Fixed Asset Policy](#).

Private use of ACC's assets

Any physical item owned, leased, or borrowed by ACC is considered an asset. These include motor vehicles, photocopiers, phones, digital devices, internet access, and stationery. As a general rule, employees should not use ACC's assets for personal reasons unless approval is obtained from the cost centre manager.

Sometimes it is impossible to avoid using a business asset for personal use. You may be asked to provide evidence that no additional cost to the organisation was incurred resulting from the personal use. Refer to [Telephony Policy](#)

Private use of ACC's suppliers

Employees can use ACC suppliers for their own personal use if they make it clear to the supplier that the arrangements are personal and the employee will pay them directly.

Employees should be moderate in their use of employee discounts, should note that these cannot be used on behalf of any third party (including family and friends), and that employee must pay in full at the time of purchase.

Some suppliers provide discounts to our employees but ACC does not take this into account when choosing suppliers. ACC selects all suppliers by following [ACC's Procurement Policy](#) and [Government Rules of Sourcing](#).

4.4 Employee support and welfare expenditure

Clothing/Corporate wardrobe

Only reception employees are entitled to a [corporate wardrobe subsidy](#). From time to time, employees who are supporting ACC initiatives may be provided a uniform to wear at an event. This becomes the property of the employee.

Long service recognition

ACC recognises employees who have reached specific milestones based upon their continuous service. See Guidelines on [Long Service Recognition](#).

Welcoming/ Whakatau/ Powhiri

A welcoming/ whakatau/ powhiri morning/afternoon tea function may be held for when a new Executive member or Head of joins ACC or moves to a different position at the same or higher level. A Head of or Chief may approve others depending on their role.

Farewells and retirements

A farewell morning/afternoon tea function may be held for permanent employees who have at least 12 months service and resign, retire or are made redundant. ACC will not contribute towards a gift or flowers for a departing employee unless they are retiring. The relevant Chief may approve exceptional circumstances to farewells and gifts. The relevant Chief may approve a gift up to \$200

A farewell function would not be held for an employee whose employment has been terminated for poor performance, inappropriate behaviour, or serious misconduct. A farewell function is not held for an employee who has moved teams- the relevant Chief may approve exceptional circumstances.

Refer to Meals, [Food and Drink](#) and [Farewells and retirements](#).

Life events

ACC may offer an expression of support or sympathy and cover the cost of flowers or a gift basket, up to the value of \$80 in the following cases:

- On the occasion of an employee's serious illness or accident
- A bereavement of an employee or employee's immediate family such as parent or child
- A birth of an employee's baby

A pre-approval is required from the Cost Centre Manager before the expense is incurred and should be arranged by the line manager of the individual receiving the gift.

Gifts for other events (including engagements, weddings, birthdays, Easter and Christmas) will not be paid for by ACC.

Employee recognition

In addition to the annual performance review cycle processes, one-off recognition and non-cash rewards may be given, usually up to \$50. Vouchers may be given to employees at the discretion of the manager, and can be obtained through the gift station procedures outlined at [Reward your employees](#)

Employee functions and team building

Team morning/ afternoon teas and team building may be used as a form of non-monetary recognition or achievements for the team. Team building activities should be up to \$30 (incl GST) per head on an annual basis and within approved budgets. Any expense over this amount must be pre-approved by the by the relevant Chief.

Employee/event sponsorship

Sponsorship is support of an event, activity, person, or organisation financially or through the provision of products or services. Refer to ACC [Sponsorship Policy](#) for guidance.

4.5 Contributions and gifts to external parties

Donations

A donation is a payment of money or provision of goods or services by ACC. A donation is voluntary and the external organisation has no expectation of receiving goods or services from ACC. All donations must be pre-approved by the Chief Financial Officer or Chief Executive. A donation is made to a recognised organisation and not to an individual nor in cash.

Koha/Meaalofa

Koha/meaalofa is an unconditional gift given and not a payment for providing goods or services received for unsolicited services. Koha/meaalofa may be given when ACC is represented at a Māori tangi or Pacific funeral.

Koha/meaalofa criteria:

- maybe given in cash
- up to \$200: cost centre manager and local cultural advisor's prior approval
- greater than \$200 requires Chief Financial Officer or Chief Executive approval

Gifts to external parties

Gifts may be given to show appreciation to individuals, groups or organisations who have provided a service at no charge, such as training, consultations or customer testing. Alcohol may not be provided as a gift. Prizes may be given to injury prevention initiatives.

These must be in line with the recommended amounts.

Gifts and Gratuities

Our people are occasionally offered a gift or gratuity from a supplier, provider or client. We must not receive or solicit gifts or gratuities from a third party for the performance of our role. As members of the public sector, our people must ensure any offer of a gift or gratuity is managed in a way that maintains the integrity and transparency of ACC and our people. This policy applies to gifts and gratuities offered to individuals, groups, or ACC as a whole, from any third party, including clients, treatment providers, preferred suppliers and other individuals or organisations.

No gift or gratuity is to be accepted from prospective suppliers who are actively tendering for the provision of goods and services.

Money must never be accepted as a gift or gratuity.

Gifts and gratuities include, but are not limited to the following due to the principle of private benefit:

- gift vouchers; goods; services; meals or other hospitality
- tickets to events (eg, sporting, musical or theatrical)
- prizes won as a result of incurring some expense on behalf of ACC
- free or discounted travel or accommodation, which includes discounted travel and accommodation for seminars)
- any other reward or benefit

If an employee is offered a gift, gratuity or money they should consult with their manager

All gifts must be recorded monthly in a register managed by the team administrator, approved by the Chief Officer and forwarded to [Procurement](#).

Exceptions:

Morning/afternoon teas and token gifts of appreciation, such as branded pens, and where the individual value is less than \$10 per person, may be accepted.

Such gifts should only be accepted where they:

- do not, or do not appear to, place the recipient under any obligation
- are not, or can not be interpreted as, a reward for preferential treatment.

Note that caution should be exercised where these are offered by a prospective supplier in the run up to, or during, a tender process.

Refer to [Gifts and Gratuities procedure](#).

4.6 Payment Methods

Payment methods are not a type of sensitive expenditure, however care must be taken to ensure sufficient documentation is retained to support the incurring and accounting of the expenditure.

Purchasing Card payments

Purchasing cards are issued by ACC's approved bank

- to purchase low dollar value good and services with suppliers where ACC has no preferred supplier arrangement.
- to employees who are permanent employees or on a fixed term contract of at least six months.

Rules:

1. The card holder is the only person authorised to use their card.
2. A Purchasing Card holder must never disclose their card's personal pin number to others.
3. Cash advances are not allowed
4. No personal expenditure may be charged to the ACC purchasing card

Purchasing cards are to be returned and cancelled when the cardholder is no longer employed by ACC. Purchasing cards that have not been used for a period of six months will be reviewed and cancelled if necessary.

Refer to [Purchasing Card procedures](#)

Invoice payments:

Where payments are made through ACC's Financial System, in addition to meeting normal invoice procedures the following details must be recorded:

- the full name of the recipient(s) being paid
- Clearly state the reason the expenses were incurred
- State the type of goods or services

Reimbursing cash payments

Employees will be reimbursed for actual and reasonable business expenses that they have paid from their personal funds on ACC's behalf.

All expenses over \$50 must be accompanied by tax invoices. If tax invoices are unavailable for expenses of \$50 or less, they must be accompanied by appropriate documentation and approved by the line manager. Expenses will be paid fortnightly into the employee's bank account via the HR payroll system. Cash reimbursements must be claimed within three months.

If an employee has a financial interest or there is a [conflict of interest](#) with the supplier the employee must declare this to the line manager before reimbursement can be made.

Refer to [Cash reimbursement procedures](#)

5 Accountabilities

Board responsibility for finances is set out in the ACC Board Governance Manual. This acknowledges that the Board plays a lead role in setting a clear strategic direction for the organisation; oversees the organisational governance framework and standards; ensures achievement of ACC's strategic and governmental objectives and approves ACC's annual business and capital plans. The Board delegates most of its day-to-day operational responsibilities to the Chief Executive, who delegates many of those responsibilities to the Executive.

The Executive is responsible for the leadership and management of the organisation and is accountable for ensuring that ACC achieves its goals.

The Chief Financial Officer has overall responsibility and accountability for the operation of this policy. Monitoring and oversight activities will be undertaken to assess the effectiveness of this policy

Managers approve sensitive expenditure:

- only when the person approving the expenditure is satisfied that the principles and rules have been adequately met;
- before the expenditure is incurred, when practical;
- only when an approved budget and delegated authority exist;
- by a person senior to the person who has incurred the expenditure.

If these conditions are not met, the expenditure should not be approved.

6 Responsibilities

Role	Responsibility
Employee	<p>Comply with the policy, procedures and guidelines</p> <p>Provide accurate, detailed payment transaction details for cash expense, purchasing card and invoice transactions</p> <p>Apply for cash reimbursements within three month of incurred cost</p> <p>Accurately enter their expenses in a timely manner to ensure the manager can approve and the expense is paid promptly</p> <p>Ensure the appropriate documentation tax receipts and/or invoices are attached to the expense claim, and obtain copies if receipts are misplaced or lost if over \$50</p> <p>Must not allow another person to use Purchasing Card</p> <p>Must not approve their own expense</p> <p>Report any breaches of this policy. Section 9 sets out how to do this.</p>
Travel Arrangers	<p>Book travel using ACC's preferred provider; to ensure best available fares are booked; and maintaining appropriate records.</p> <p>International Travel Arrangers manage Trans-Tasman and International travel and accommodation</p> <p>Domestic Travel Arrangers manage domestic flights, accommodation and rental vehicles</p>
Coding Administrator	<p>Provide accurate, detailed payment transaction details</p> <p>Ensure teams monthly accruals are recorded</p>
Line manager	<p>Approve cash expense and purchasing card transactions to ensure timely reimbursement of expenses</p> <p>Decline expenses that do not comply with this policy and procedures and discuss with the employee.</p> <p>Request reimbursement, where required, when a purchase has been made outside of policy</p> <p>Immediately question any unusual transactions with the employee</p> <p>Only approve legitimate business expenses supported with relevant documentation</p> <p>Approve gifts received team members</p> <p>Ensure expense claims for \$50 or more have tax invoices with receipts attached</p>
Purchasing Card and Cash Expense Administrator	<p>Set up new employees in the Expense Management System</p> <p>Identify any breaches of policy and forwarding to relevant personnel</p>

	<p>Manage the Expense Management System information</p> <p>Administer and update changes to employees' profiles</p>
Cost Centre manager	<p>Approve expenses other than cash expense and purchasing card transactions</p> <p>Endorse Trans-Tasman and international travel</p> <p>Approve exceptions for domestic travel and accommodation</p> <p>Endorse Koru Club memberships</p> <p>Gifts to external parties in line with recommended amounts</p> <p>Approve monthly gift register</p>
Heads of	Approve Welcoming/ Whakatau/ Powhiri
Group - Chief Officer(s)	<p>Set expectations and manage policy</p> <p>Approve purchase of alcohol</p> <p>Approve exceptional circumstances for farewell gifts for non-retiring employees</p> <p>Approve Koru Club memberships</p> <p>Approve Cost Centre Manager domestic travel and Trans-Tasman travel</p> <p>Endorse international travel</p> <p>Approve Welcoming/ Whakatau/ Powhiri</p> <p>Approve gift up to \$200 in exceptional circumstances</p> <p>Approve a farewell function for an employee who is moving teams</p> <p>Approval of greater than 1 mit for team building</p> <p>Approve the group's gift register</p>
Chief Financial Officer	<p>Approval of Donation</p> <p>Approval of Koha greater than \$200</p>
Chief Executive	<p>Set expectations and manage policy</p> <p>Approve Group – Chief Officer travel and approve International Travel</p> <p>Approval of Donation</p> <p>Approval of Koha greater than \$200</p> <p>Approve gift to external party where it is, in aggregate, greater than \$500</p> <p>Approve Chief's gift register</p>
Procurement Services	Manage the operational component of this policy and the relationship with our preferred suppliers.
Finance and Performance Group	<p>Second level approval after line manager for cash expenses</p> <p>Review cash expense, purchasing card and invoice transactions</p>
Risk and Actuarial Group	<p>Audit financial policies and procedures</p> <p>Arrange for external auditors when required</p> <p>Report outcomes to the Chief Financial Officer</p>

7 Monitoring and oversight

Regular reporting will be provided to the Executive Leadership and to the RAAC as needed on sensitive expenditure and the level of policy compliance. The five lines of defence outlined below work together

with the objective of ensuring compliance with relevant policy and procedures and protect ACC's reputation.

Line of Assurance	Monitoring and oversight activities:
1st Line Our people People managers/ cost centre managers	<ul style="list-style-type: none"> • Embedding financial responsibilities in the business • Ensure compliance with the sensitive expenditure policy, principles, procedures and delegations framework • Ensure line managers review and approve all expenditure in line with policy and principles
2nd Line Finance and Performance Group	<ul style="list-style-type: none"> • Cash expenses are reviewed and approved by Finance and Performance Group, following the approval of the line manager • Purchasing card transactions are reviewed by Finance and Performance Group and anomalies are followed up • Invoice payments are reviewed for appropriateness by Finance and Performance Group • Provide advice to the business on sensitive expenditure issues • Report anomalies to the Chief Financial Officer
3rd Line Assurance Services External Audits	<ul style="list-style-type: none"> • 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 • Work closely with ACC's enterprise Risk and Compliance team who provide second-line assurance role
4th Line	<ul style="list-style-type: none"> • Approve this policy and appropriate expenses
5th Line	<ul style="list-style-type: none"> • Approves Chief Executive expenses

8 Breaches of Policy

Transactions are monitored regularly by the Finance and Performance Group and to ensure compliance with this policy.

The Head of Procurement and the Chief Financial Officer have the authority to disallow any expenditure considered to be unreasonable or not compliant.

Complying with all policies and procedures is a requirement outlined in the Code of Conduct.

Breaches of this policy will be reported to the Chief Financial Officer and may result in disciplinary action. Behaviour or actions that are investigated and found to be in breach of the [Code of Conduct](#) may result in disciplinary action.

If you would like to make a confidential disclosure regarding sensitive expenditure, refer to [Making a protected disclosure](#). Alternatively, you can contact [Procurement](#).

9 Contacts

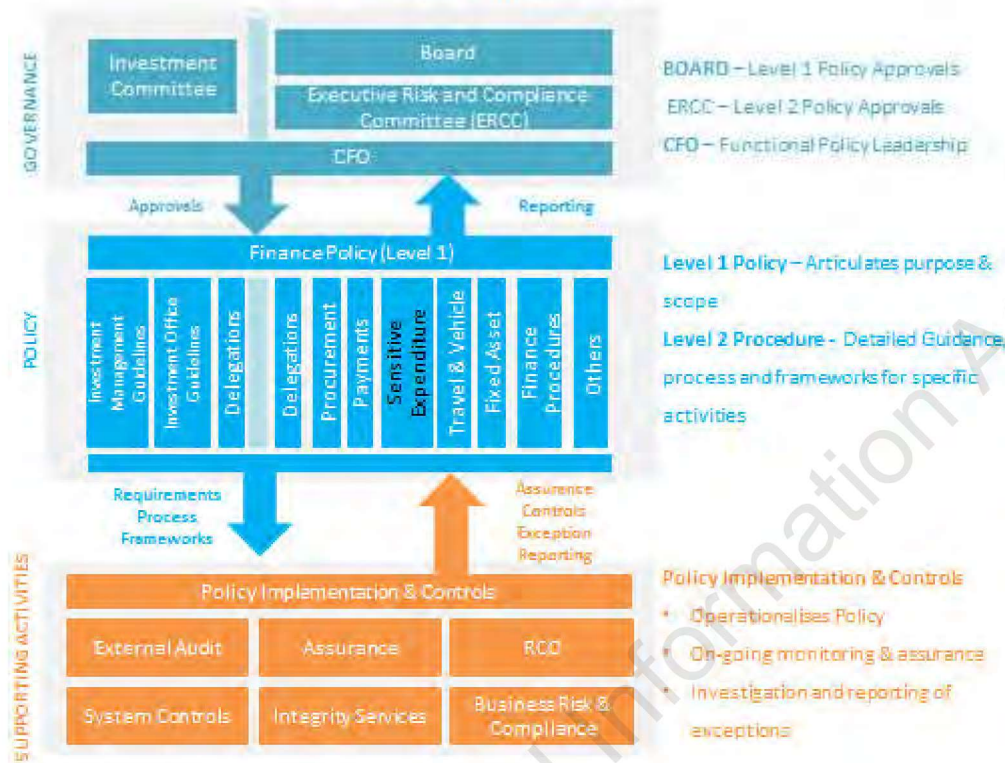
Contact the Manager, Business Improvement and Support in the Procurement Services team, regarding this policy.

Appendix: Finance Policy System Diagram

An overview of ACC's Financial framework is detailed below and shows how key aspects work together to achieve financial objectives as delivered by this policy.

Released under the Official Information Act

FINANCIAL POLICY LANDSCAPE



Released under the Official Information Act



Health, Safety and Wellbeing Policy

POLICY NUMBER	3.0.0
TOPIC	Health, Safety and Wellbeing Policy
OWNER	[REDACTED] Head of Health, Safety and Wellbeing Talent
DATE APPROVED	30 September 2020
APPROVER	ACC Board
DATE OF NEXT REVIEW	September 2021

1 Policy Statement

ACC will, so far as is reasonably practicable ensure that the work we do and direct is healthy and safe for all involved, and that the wellbeing of our people is supported.

2 Objective

This policy guides all people who direct or undertake the work of ACC, including our Executive and Enterprise leaders, People Leaders, Elected Health and Safety Representatives and all our people to achieve a healthy and safe work environment and support the wellbeing of our people.

3 Scope

This policy applies to all ACC employees and other people who carry out work in any capacity for ACC.

- “Our people” are people directly employed by ACC on a permanent, fixed term or casual basis.
- “Other people” who carry out or may be affected by our work includes our contractors, our providers (and their people), our clients and our visitors.

4 Policy Principles and Standards

4.1 We all have a part to play in keeping each other healthy, safe and well by:

- Supporting our people to understand their roles and responsibilities, and to develop their capabilities, in relation to health, safety and wellbeing.
- Maintaining processes to encourage and enable our people and their representatives to engage and participate in health, safety and wellbeing at ACC.
- Training and supporting people who take on specific health, safety and wellbeing leadership responsibilities in addition to their main role to ensure they can contribute with skill and confidence.
- Supporting our leaders to develop effective skills to manage the risks in their workplace, and contribute to the delivery and ongoing improvement of health, safety and wellbeing across ACC.
- Developing our Executive and Enterprise leaders to ensure they effectively lead and promote health, safety and wellbeing across ACC.

4.2 We actively manage risks that could harm us or others by:

- Identifying our risks and eliminating or minimising these so far as is reasonably practicable.
- Regularly reviewing the ongoing effectiveness of our risk management controls.
- Identifying any groups who may be more at risk than others and ensure our control measures specifically address their increased risk exposure or likelihood of harm.
- Supporting our providers and other partners to develop their management of health and safety risks through the procurement process and ongoing relationship management and service delivery.
- Embedding the management of health, safety and wellbeing risks into all our business decisions and operations by eliminating or controlling risks as early as possible in the planning and design or change processes.
- Ensuring an effective system is in place for reporting incidents and responding appropriately, focusing on resolving the issues raised through the reports.

4.3 We work together to support our people and our communities by:

- Using our experience, insight and information to understand the needs of our people and identify opportunities to improve our health, safety and wellbeing outcomes.
- Developing initiatives in collaboration with our people to ensure the focus is on what is important for them in their workplace.
- Sharing our initiatives with other people who do work for ACC, and our wider communities where appropriate.

- Supporting our people to be injury prevention ambassadors through the communication and delivery of external ACC injury prevention initiatives.

4.4 We monitor how we're doing and keep improving by:

- Identifying and collecting good quality and timely information to identify risks and understand the drivers of harm in our workplace and in the work other people do on our behalf.
- Sharing our information and insight with our people and other people where appropriate to improve health, safety and wellbeing outcomes within ACC, across government, our provider network, and other sectors.
- Providing timely and accurate information to support the due diligence activities of the Board.
- Celebrating our achievements and being transparent where we fail to meet our performance expectations.

5 Accountabilities

The Board's responsibility for health, safety and wellbeing is set out in the ACC Board Governance Manual. As officers of ACC, Board members must exercise due diligence to ensure ACC complies with its obligations and primary duty under the Health and Safety at Work Act.

The Board exercises its due diligence by overseeing the four key elements in health and safety governance. These are: Policy and Planning; Delivery; Monitoring; and Review.

To support the Board, our Executive and Enterprise Leaders will:

- Act with due diligence and skill to ensure the work ACC does and directs is healthy and safe for all involved and that the wellbeing of our people is supported
- Actively seek information about ACC's health, safety and wellbeing matters and stay informed and up to date
- Understand the work ACC carries out, in particular the work under their area of control, and the hazards and risks to people's health, safety and wellbeing associated with that work
- Ensure ACC, in particular the area under their control, is sufficiently resourced to effectively manage health, safety and wellbeing risks.

6 Responsibilities

Role	Responsibilities
Our people	<ul style="list-style-type: none"> • Take reasonable care of their own health, safety and wellbeing and ensure that their actions don't cause harm to themselves or others • Comply with any reasonable instructions, policies or procedures on how to work in a safe and healthy way

	<ul style="list-style-type: none"> • Report health and safety concerns or suggestions for improvement to their manager or elected Health and Safety Representative and record any incidents in HR Self Service.
Other people	<ul style="list-style-type: none"> • Where this policy applies to other people who are doing work (or planning on doing work) for or on behalf of ACC, ACC and the other people or their employer will, so far as is reasonably practicable, work together to ensure the work the other people do is healthy and safe. • Where Other People are in our workplaces, they must: <ul style="list-style-type: none"> ○ take reasonable care and ensure that their actions don't cause harm to themselves or others ○ comply with instructions on how to work in a safe and healthy way ○ report any incidents to their supervisor, host or other ACC person.
Elected Health and Safety Representatives	<ul style="list-style-type: none"> • Advocate for the people they represent and provide health, safety and wellbeing information and advice to those people • Attend and participate in training and health and safety engagement meetings • Work with People Leaders and others to ensure the work we do and direct is healthy and safe, and that the wellbeing of our people is supported • Where work is unsafe and improvements to make it safe cannot be identified, cease unsafe work and/or issue improvement notices
People Managers	<ul style="list-style-type: none"> • Identify and manage risks and hazards arising from the work under their control, and take steps to eliminate or minimise those risks • Ensure their people are appropriately trained and supported in relation to their health, safety and wellbeing responsibilities and our policies and procedures • Respond, investigate, and actively manage incidents logged by their people on HR Self Service • Model and promote healthy and safe work and support the wellbeing of their people.

Head of Health, Safety and Wellbeing	<ul style="list-style-type: none"> • Ensure the health, safety and wellbeing management system is fit for purpose, effectively implemented, regularly reviewed and continuously improved • Ensure that change management processes provide assurance that health, safety and wellbeing risks have been considered in the design of processes, products, programmes and projects • Design and deliver injury prevention, healthy work and wellbeing initiatives for ACC people • Provide health, safety and wellbeing representatives with necessary information about health, safety and wellbeing systems and performance • Consult with and seek recommendations from health and safety representatives through the regional and organisational health and safety committees • Monitor the health, safety and wellbeing performance of the organisation, review information and identify continuous improvement opportunities.
Chief Talent Officer	<ul style="list-style-type: none"> • Develop the high-level health, safety and wellbeing strategy and policy • Develop targets that enable the organisation to track performance in implementing the health, safety and wellbeing strategy and policy • Ensure there is an appropriate health, safety and wellbeing management system in place to meet ACC's health, safety and wellbeing obligations • Ensure ACC is sufficiently resourced to meet these obligations.
Executive and Enterprise Leaders	<ul style="list-style-type: none"> • Visibly demonstrate their commitment to health, safety and wellbeing through their actions, including regularly engaging with their people about health, safety and wellbeing matters that are important to them.
Board	<ul style="list-style-type: none"> • Provide effective governance and leadership of health, safety and wellbeing for ACC.

7 Monitoring and Oversight

This policy has been designed to assist with the management of the Enterprise risk that “We fail to take reasonable and practicable steps to prevent harm to employees or third parties”. The responsibilities, according to the five lines of assurance model, are set out below.

Line of assurance	Responsibility
1st Line Our people	<ul style="list-style-type: none"> • Our people are in control of their day to day activities, recognising and managing health, safety and wellbeing risks. • Understand the health, safety and wellbeing risks and controls associated with their work • Manage risks by following and operating within our health, safety and wellbeing policy and procedure

	<ul style="list-style-type: none"> • Identify opportunities and make recommendations for improvement either directly or through health and safety representatives, or cease unsafe work where improvements cannot be identified • Consider health, safety and wellbeing risks when making decisions and ensure any identified risks are appropriately managed.
2nd Line Health, Safety and Wellbeing Team	<ul style="list-style-type: none"> • The Health, Safety and Wellbeing function within Talent provides oversight and specialist subject matter expertise across the business. • Keep policies up to date and fit for purpose • Work across the organisation to educate, inform and design processes for employee engagement; risk management; injury prevention, healthy work and wellbeing initiatives; and monitoring, understanding and reporting in relation to the management of health, safety and wellbeing • Monitor and regularly review the health and safety system is being applied and is working effectively across the business • Gather insights relating to health, safety and wellbeing risks, policy and control environment, and incidents that inform reporting to the Executive and Board.
3rd Line Assurance Services	<ul style="list-style-type: none"> • Assurance Services independently review the overall reliability of the health, safety and wellbeing risk management processes and performance. • Assess and audit the health, safety and wellbeing control environment, policy and performance governance and accountability.
4th Line Executive	<ul style="list-style-type: none"> • The Chief Executive and Chiefs have overall responsibility for building and maintaining robust framework for managing health, safety and wellbeing risks • Identify and manage health, safety and wellbeing risks to our strategic intentions, business strategy and operations • Manage within our health, safety and wellbeing risk controls and report to the Board on health, safety and wellbeing risk status management • Have responsibility for health, safety and wellbeing policies, processes and compliance • Have overall responsibility for risks relating to business objectives.
5th line Board	<ul style="list-style-type: none"> • Have overall responsibility for ensuring health, safety and wellbeing risk management is in place • Ensure governance of effective risk management policies and processes • Set risk parameters and approve health, safety and wellbeing policy • Review health, safety and wellbeing management and risk reporting and assess risk status and targets.

8 Breaches of policy

Complying with all policies and procedures is an expectation outlined in the 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.

9 Contacts

Contact the [Health, Safety and Wellbeing Team](#) in relation to any queries regarding this policy.

10 Definitions

Reasonably practicable

Reasonably practicable is defined in the Health and Safety at Work Act in relation to what is able to be done to ensure health and safety, taking into account and weighing up all relevant matters, including:

- (a) the likelihood of the hazard or the risk concerned occurring; and
- (b) the degree of harm that might result from the hazard or risk; and
- (c) what the person concerned knows, or ought reasonably to know, about the hazard or risk and ways of eliminating or minimising the risk; and
- (d) the availability and suitability of ways to eliminate or minimise the risk; and
- (e) after assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

11 References

Legislation and regulations

[Health and Safety at Work Act 2015](#)

[Health and Safety in Employment Regulations 1995](#)

[Health and Safety at Work \(General Risk and Workplace Management\) Regulations 2016](#)

[Health and Safety at Work \(Worker Engagement, Participation, and Representation\) Regulations 2016](#)

ACC policies

[Building security policy](#)

[Smoke-free Policy](#)

[Employee Injury Management and Rehabilitation Policy](#)

Information Security Policy



POLICY NUMBER	5.1.0
TOPIC	Information Security Policy
OWNER	██████████ Chief Information Security Officer (CISO) ██████████
BUSINESS GROUP	Technology and Innovation
AUTHOR	██████████
DATE APPROVED	02 December 2020
APPROVER	Peter Fletcher, Chief Technology and Innovation Officer
NEXT REVIEW DATE	02 December 2022

1 Policy Statement

The purpose of this policy is to ensure that ACC's information assets (physical or digital) are appropriately secured and protected from internal and external threats in the interests of the people of NZ, the NZ government and ACC customers. These information assets are essential to the operation of ACC and if they are not available, improperly accessed or disclosed, ACC can incur significant reputational, operational and/or financial loss.

In addition, ACC must comply with all legislative and NZ government requirements to safeguard and protect customer and staff privacy. Information is core to all of ACC's responsibilities and therefore this policy is also intended to ensure that the appropriate degree of access, sharing and protection of information assets will occur so as not to unreasonably restrict the utility of information assets.

2 Scope

This policy applies to:

- All employees whether permanent, short/fixed term, or seconded, and contractors
- All activities performed by, or on behalf of, or in collaboration with ACC including the creation, storage, retrieval, maintenance, sharing and transmission of all ACC information whether

physical or electronic

- All information that may be located within ACC, or provided as an external contracted service
- Any future use of information technologies that ACC may use to redefine, or repurpose, information assets

This policy is to be read in conjunction with the:

- Information Management Policy
- Information Management Standards
- Information Security Standards
- Stewards and Custodians Standard
- Guidelines and Procedures documents.

Employees, contractors, and service providers who deliberately breach this policy may be subject to disciplinary action and/or commercial remedies.

3 Policy Principles

The following principles must be adhered to for information security:

3.1 We protect our information and data against any unauthorised access

Access to our information assets, and where they are held, must be controlled. Access is only authorised based on the principle of minimum required privileges. This provides protection from accidental, malicious, or unauthorised change.

All employees, contractors and external party users must ensure that these privileges are not abused, transferred, or retained, when no longer required in the performance of their duties. Additionally, they must:

- Read, agree to, and sign a copy of the ACC162/162a Confidentiality and Information Security Agreement
- Assess and balance the risks and consequences prior to any transfer of information or data relative to the type of information or data
- Where data transfer is automated, this transfer **must** be subject to ACC's certification and accreditation requirements **prior** to any transfer.

3.2 We maintain the security and availability of our information and data

The ACC Certification and Accreditation process sets the minimum requirements for securing our IT systems based on the system's risk assessment, our information security standards, and risk appetite.

- All IT systems must be assessed via the ACC Certification and Accreditation process before it is used to hold or process any ACC information and data assets
- All certified systems must be re-assessed at least every three years, unless written exemption has been granted by the ACC Accreditation Authority
- When our people are working remotely, they must do so using an ACC certified environment and must not allow ACC information or data to be copied, saved or printed on uncertified devices.

Operational systems and application software are subject to a strict change management control system and standards which must be followed in order to meet Certification and Accreditation requirements.

Audit logs on all of our systems must be produced, maintained, and retained for an agreed period in accordance with legal, regulatory, and operational requirements. These must include but are not limited to recording user activity, exceptions and information security events.

Protecting our operational capability from the destruction of information and data assets or the loss of access to operational systems, as a result of disaster or a breach of cyber security, is critical. All operational systems and processes must have controls in place to ensure ACC can recover quickly in the case of such an event.

3.3 We meet all legislative and regulatory requirements

We hold information and data assets that are highly sensitive and protected under legislation. We must apply policy frameworks, standards and guidelines as set out in the Government's expectations for managing information and data assets.

This includes compliance with all relevant legislation, and the following Government guides:

- Protective Security Requirements (PSR)
- New Zealand Information Security Manual (NZISM).

We must also comply with the legislation and principles set out by the Government that ensure appropriate information and data is open for public access and readily available.

Appendix A lists relevant Government legislation, charters and principles.

3.4 We ensure that information security training is available for all employees

The Informat on Security Team is responsible for relevant information security training development and delivery.

This includes regular training and review, education and awareness programmes as well as critical threat awareness measures as required.

All our people and contractors must complete the mandatory elements of this training and maintain a minimum standard of security awareness when using our assets, facilities and systems.

3.5 We must report all potential, actual, or suspected, information security breaches to the Information Security Team and they must ensure these breaches are thoroughly investigated

The Information Security Team is responsible for investigating, reviewing and responding to all security breaches.

We must all co-operate with security investigations. The Information Security Team must alert the appropriate authorities immediately if threats or threat levels increase beyond acceptable levels.

The CISO and/or Information Security Team must communicate with all of our people at the earliest opportunity if they need to be aware of the increased threats, or threat levels. This communication must inform our people of appropriate measures, or actions, needed to minimise and/or eliminate the potential threats.

3.6 We will assess and assure our information security practices and resources keep pace with changes and threats as they evolve.

We acknowledge the changing environment of Information Security may require policy changes and updates on a faster timescale where technology or threats change.

Our Information Security Team must:

- Maintain their skills
- Monitor and maintain an awareness of the threat environment
- Make sure timely security advice and appropriate alerts are provided
- Work with learning and development to provide and update training resources
- When warranted increase capacity and capability to counter new and emerging threats.

Standards and procedures may be updated as required and these changes will be communicated through appropriate channels once approved.

4 Accountabilities

The Chief Executive and the Executive team are accountable for Information Security at ACC.

The Chief Executive has delegated the responsibility for ensuring organisational controls are in place in support of this policy to the Chief Technology and Innovation Officer (CTIO) in conjunction with the Chief Information Security Officer (CISO).

This policy will be formally reviewed every 2 years as per NZISM standards. ACC acknowledges the changing environment of Information Security may require policy changes and updates on a faster timescale where technology or threats change.

This policy sits with the Governance of Information Governance Group (IGG) and the Security and Privacy Advisory Group (SPAG). The policy is also aligned with the directions and oversight of the Contents and Records Advisory Group (CRAG).

5 Responsibilities

Role	Responsibility
Chief Executive	Ultimate accountability for Information Security at ACC
Chief Technology and Innovation Officer (CTIO)	Has overall responsibility for information and cyber security matters in ACC
Chief Information Security Officer (CISO)	Is responsible for the management for cyber security strategy and governance.
Security and Privacy Advisory Group (SPAG)	Will hold the delegated responsibility for any iterative updates that are deemed required to secure the ACC environment outside of the normal 2-year policy review cycle. These changes will be documented and subject to approval by the CTIO. These changes will be communicated as appropriate to all relevant parties
Information Technology Security Manager (ITSM)	The ITSM is responsible for managing ICT security and ICT operational risks on a day-to-day basis. All related ICT security incidents are centrally managed and reported to the Chief Information Security Officer and where necessary the Chief Technology and Innovation Officer
Information Security Team	Monitors compliance with this policy working with users to ensure the safety and security of ACC information
Managers	Are responsible for ensuring that their team members are aware of and understand this Policy, and that all associated requirements are met by their team members in the performance of their duties
Our people, providers and suppliers	Are to make sure they know their responsibilities and comply with this policy Read, comprehend and comply with the requirements outlined in the ACC162/162a Confidentiality and Information Security Agreement
Information Stewards and Custodians	Are responsible for ensuring that information assets, for which they are accountable, are appropriately classified and protected from compromise and misuse
Talent's People Development Team	Are responsible for including the ACC162/162a Confidentiality and Information Security Agreement within standard contracts of employment and the staff induction programme

6 Monitoring and oversight

The monitoring and oversight of privacy follows the five lines of assurance model (LOA).

LOA:	Role	Monitoring & Oversight
1st Line	Employees and People Managers	<p>All people managers monitor the completion of information management modules and training.</p> <p>All employees remain alert to potential breaches of the Policy and report potential and actual breaches to their manager.</p> <p>All people managers ensure that breaches brought to their attention are documented, and notification of the breach is provided to the owner of the Policy within five days of the breach occurring.</p> <p>From time to time we deliberately take actions contrary to a policy's provisions (corporate policy exceptions). When people managers are responsible for a corporate policy exception, the people managers ensure that the exceptions are agreed either using the process in the Policy or by agreement in writing from the Policy owner.</p>
	Group Risk and Compliance Manager and/or Advisor	<p>Supports employees/groups to determine whether events constitute actual breaches of the Policy.</p> <p>Escalates breaches to the Group's Leadership Team and Chief when appropriate.</p> <p>Updates risk registers as required.</p>
	Policy Owner	<p>The Policy Owner ensures that the Group (and other parts of ACC if applicable) respond appropriately to Policy breaches and requests for exceptions.</p>
2nd Line	Enterprise Risk Team	<p>Performs periodic oversight activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches.</p> <p>Reports to the Executive and the Board on the outcomes of such activities.</p>
	Enterprise Data Information and Security (EDIS) team	<p>Provide oversight of all information management aspects in this policy and subject matter expertise to staff and management when required</p> <p>Regularly review and report to ensure the intention of the policy is being honoured</p>

LOA:	Role	Monitoring & Oversight
		<p>Carry out periodic audit and assurance activities on information management practices along with the Enterprise Risk and the Privacy team</p> <p>Supports employees to determine whether events constitute actual breaches of the Policy.</p> <p>Escalates breaches to the Group's Leadership Team and Chief when appropriate.</p> <p>Supports the oversight of our information security practices and decision making via the Information Governance Group and sub governance groups</p>
3rd Line	Internal Audit (and external providers)	<p>Performs periodic audit activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches</p> <p>Reports to the Executive and the Board on the outcomes of such activities.</p>
4th Line	Executive	<p>Ensures each Group has sufficient emphasis on risk management and meeting compliance obligations.</p> <p>Ensures effective processes and monitoring are in place to meet compliance obligations for the Policy.</p> <p>Acts in an appropriate and timely manner in response to reports received that alert the Executive to opportunities to improve Policy compliance activities.</p>
5th Line	Board	<p>Responsible for approving any material changes to the Tier 1 Policies, including text related to monitoring and oversight of compliance with the Policy.</p> <p>Acts in an appropriate and timely manner in response to reports received that alert the Board to opportunities to improve Policy compliance activities.</p>

7 Breaches of Policy

Complying with all policies, standards and procedures is a requirement outlined in the 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 ACC's [Code of Conduct](#) for further information.

8 Contacts

For any enquiries about issues of interpretation or management of the policy please contact the

Information Security Team - infosec@acc.co.nz

9 Appendix A

Legislation, Policy, Charters, and Standards

Subordinate Policies and Standards
Use of the Internet Policy (Tier 3) Email and Instant Messaging Policy (Tier 3) Information Management Standards (omnibus document) Information Security Standards (omnibus document) Stewards and Custodians Standard
Associated Technology Policy and Standards
Information Management Policy (Tier 1) Privacy Policy (Tier 2) Telephony Policy (Tier 3) BYOD Policy (Tier 3) Modern Device Standards Vendor Device Standard
Related Acts and Codes
Accident Compensation Act 2001 Privacy Act 2020 Public Service Act 2020 Health Information Privacy Code 1994 Public Records Act 2005 Health Act 1956 New Zealand Public Health & Disability Act 2000 Tax Administration Act 1994 Copyright Act 1994 Official Information Act 1982 Contract and Commercial Law Act 2017 Evidence Act 2006 Financial Reporting Act 1993 Public Finance Act 1989 and Public Finance Amendment Act 2004 Resource Management Act 1991 and Resource Management Amendment Act 2005 State-Owned Enterprises Act 1986 Health and Safety in Employment Act 1992 New Zealand Public Health & Disability Act 2000

10 Appendix B - Definitions

Word/Phrase	Explanation
-------------	-------------

Information Security	<p>Information Security is a component of Risk Management and is defined by the Government Communications Security Communications Bureau (GCSCB) as measures relating to the confidentiality, availability and integrity of information.</p> <p>Protection measures can be:</p> <ul style="list-style-type: none"> • Procedural, such as use, handling, transmission and access restricted to suitably cleared employees. • Physical, such as storage and access to work areas • Technical, such as encryption and firewalls.
Information Assets/Our Data/Our Information	<p>An information asset is any information or related equipment that has value to ACC including:</p> <ul style="list-style-type: none"> • Printed documents and papers • Electronic data • The software or ICT systems and networks on which information is stored, processed or communicated by or on behalf of ACC • The intellectual information (knowledge) acquired by individuals • Physical items from which information regarding design, components, or use could be derived.
Confidentiality	<p>In information security, confidentiality relates to ACC data and other information assets. Access to these must be confined to people properly authorised. For example, this could mean using a strong password on your computer, shredding sensitive documents and locking filing cabinets.</p>
Integrity	<p>From an information security perspective, data integrity means keeping, maintaining and assuring the accuracy and completeness of data over its entire life cycle. This means watching out for and mitigating against alterations through malicious action, simple innocent mistakes, through to natural disasters.</p>
Availability	<p>For any information or information system to serve its purpose, the information must be available when it is needed. This means that the information systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly to agreed standards.</p>
Privacy	<p>There is an obvious overlap between information security and privacy. Privacy is covered in detail in the ACC Privacy Policy. This policy this</p>

Email Standard

Objective

ACC is committed to ensuring that all information, records and data are identified, filed, stored and disposed of appropriately. This ensures that ACC staff and customers have confidence in the integrity of the information and helps reduce risk to ACC.

Email is a communication tool that is used everyday to communicate, collaborate and share information internally and externally. Email mailboxes should be used as a temporary store only and business emails must be kept in the appropriate recordkeeping systems

Scope.

This policy and standard applies to all email created, received and managed by the organisation in the conduct of its affairs, by staff of ACC and its affiliated organisations. This includes all work done by ACC, or on behalf of ACC by contractors.

The standard covers the use of email and any attached files, pictures, or other content that may be embedded within sent or received email. This policy also covers any email sent or received internally within or external to ACC.

Storage

Email is **not** the appropriate storage repository for business records. Email is a communication tool and should be used as a temporary store only. Business email must be kept in the appropriate information and recordkeeping business systems.

Examples of business records are:

- Evidence of decisions and processes undertaken by ACC
- Policy or development information
- Personal information
- Significant projects
- Financial information
- Messages that contribute to a greater understanding of significant documents or events
- Formal communications between staff, including minutes for action plans and submissions

Do **not** keep business emails in your personal drives ie: folders in your email, H:drive or print out into hard copy. All substantive email should be stored in core information and recordkeeping business systems ie: Shared drives, EOS.

Retention and Disposal

Email will be disposed of according to legislative requirements. ACC's approved Corporate Retention & Disposal Schedule will be applied. That is:

- Up to 1 year of emails will be visible in staff email mailboxes
- Emails older than 1 year will be moved into archive store where they can be retrieved
- Disposal after 10 years for agreed business units that commonly engage in high-value communications
- All other emails will be disposed of after 7 years

Roles and responsibilities

Staff	<p>Must capture emails of high value in a recordkeeping system.</p> <p>Must be aware of and adhere to the Email Policy and Standard</p>
Managers	<p>Must ensure the Email Policy and Standard and are known and followed by staff</p> <p>Must demonstrate good email behaviours</p> <p>Must address email issues with the appropriate staff</p>
Contractors, Vendors and persons acting on ACC's behalf	<p>Must adhere to the Email Policy and Standards and ACC's Code of Conduct</p>
Information and Digital Tools	<p>Must maintain and administer the Email Policy and Standard.</p>

Released under the Official Information Act 1982

Media Policy

Contents

1. [Policy Statement](#)
2. [Objective](#)
3. [Scope](#)
4. [Policy Principles](#)
5. [Accountabilities](#)
6. [Responsibilities](#)
7. [Monitoring and Oversight](#)
8. [Breaches of Policy](#)
9. [Contacts](#)
10. [References](#)
11. [Version Control](#)

1. Policy statement

The Media and Social Media Policy (the Policy) defines how ACC uses social media, and manages its relationships with traditional media. It sets out the principles of engagement that govern all interactions, and is designed to protect our people, and prevent them from bringing ACC into disrepute inadvertently or intentionally.

2. Objective

The objective of this policy is to protect ACC's standing, and enhance our reputation, by setting appropriate standards and instructions for interacting on social media and with traditional media. ACC uses both avenues to inform and interact with the public. What we say and how we act can have considerable influence on people's perceptions of us, which in turn flows through to our public trust and confidence measures.

3. Scope

This policy applies to all people (permanent, temporary, and casual employees, and contractors) working on behalf of ACC.

4. Policy principles

The principle of enhancing and protecting ACC's reputation and brand underpins this policy. All communications with media or through social media must adhere to the strategic direction of ACC, and be done in a professional, courteous, and timely way.

4.1 We respond promptly to media enquiries

We respond quickly to media queries to limit potential reputational damage caused by adverse or incorrect media coverage.

Subject matter experts and organisational leaders are responsible for helping the Media team prepare informative and timely responses to media, so that we can effectively manage ACC's reputation. Requests for assistance must be given priority.

4.2 The media team oversees all contact with media

All communications – proactive or reactive – with media must be discussed in advance with the Media team, or the Manager External Engagement.

Media visits to our offices require pre-approval from the External Engagement team.

4.3 Only authorised employees can express views on behalf of our organisation

Only employees who are authorised to do so may speak to media on behalf of ACC. In all circumstances, any contact by media must be directed to the Media team or, if unavailable, the Manager External Engagement.

Employees can express their opinions in their own time on social media channels but they must not represent ACC in any form – that is the role of ACC's official social media accounts. Employees can support ACC on social media channels by liking, sharing, or engaging with the communication.

Only ACC's official social media accounts should answer questions relating to ACC or its programmes. Any employees who are asked questions on social media should direct people to those accounts, rather than providing advice in their personal capacity. This is to protect the reputation of ACC and to protect the employee.

Any social media channel representing ACC must be approved by the Manager Channel Engagement, and then managed by the External Engagement team. This is to protect ACC's reputation, and to maintain consistency of standards.

Any advertising using any social media channel must be approved by the Manager Channel Engagement. This includes partner advertising where ACC is acknowledged.

4.4 Our employees must not disclose confidential information

Requests for information that is confidential must be referred to the Governance Group Office, so the request can be considered within the provisions of the Official Information Act and/or the Privacy Act.

5. Accountabilities

The Chief Customer Officer is accountable, through the Head of Communications and Engagement, for ensuring this policy is implemented.

6. Responsibilities

Role:	Responsibility
Board and Executive	<ul style="list-style-type: none"> Support the implementation of this Policy.
Policy Owner	<p>The Policy Owner is accountable for the following, however responsibility may be delegated:</p> <ul style="list-style-type: none"> Ensure policy content is accurate, relevant, and complete and aligned with this framework. Designate policy leads to manage the writing and updating process Oversight of adherence to the policies & procedures Support policy leads with addressing any noncompliance issues.
Policy Lead	<ul style="list-style-type: none"> Ensure policy content is accurate, relevant, and complete and aligned with this framework. Ensure that policy reflect applicable obligations, rules, standards and codes. Ensure that document support to policy is available and also reviewed whenever changes are made (e.g. procedures, guidelines, forms, templates etc.). Ensure that sign-off approval is obtained from the policy owners and approving authority. Monitor effectiveness and adherence to policies and procedures. Ensure that policies are communicated and training is provided to all employees who need to comply with them.
	<ul style="list-style-type: none"> Ensure the Policy Owner and Author

Subject Matter Experts (SMEs)	changes that affect a policy or procedure.
External Engagement team	The External Engagement team, via the Principal Media AdviserMedia Engagement Manager and the Manager Channel Engagement, will ensure that all supporting operational guidance, advice, monitoring and reporting are in place and available.
ACC employees	<p>Employees are responsible for ensuring that they comply with this policy and work with the External Engagement team as required</p> <p>All ACC employees are responsible for their own conduct on social media channels.</p>
People managers	People managers are responsible for ensuring all employees (permanent, temporary and casual employees, and contractors) are aware of, understand, and comply with this policy. They are also responsible for ensuring the External Engagement team approves all media and social media communications prior to sign off.

7. Monitoring and oversight

1.1 Lines of Assurance:	1.2 Role
-------------------------	----------

1.1 Lines of Assurance:	1.2 Role
1.4 1st Line 1.5	Employees and People Managers Group Risk and Compliance Manag and/or Advisor (If applicable) Policy Owner
1.6 2nd Line 1.7 1.8	Enterprise Risk Team

Released under the Official Information Act 1982

1.1 Lines of Assurance:	1.2 Role
1.9	Specialist Functions
1.10 3rd Line 1.11 1.12	Internal Audit (and external provide
1.13 4th Line 1.14 1.15	1.16 Executive

Released under the Official Information Act 1982

1.1 Lines of Assurance:	1.2 Role
1.17 5th Line 1.18 1.19	1.20 Board

[1] The "Policy Breach Template" can be used for this purpose but is not mandatory.

8. Breaches of Policy

Complying with all policies and procedures is a requirement outlined in the 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](#) (hyperlink) for further information.

9. Contacts

The Manager, Media Engagement, and Manager Channel Engagement are the primary contacts for this policy. The Manager External Engagement is the secondary contact.

10. References

This policy should be read in conjunction with ACC's [Code of Conduct](#), and policy procedures relating to Brand; Official Information Act requests; internet access, email, and instant messaging; and Conflict of Interest.

Where ACC standards are not specified in this policy, ACC staff should refer to the Media or Channel Engagement teams.



Privacy Policy

POLICY NUMBER	5.3.0
TOPIC	[REDACTED]
OWNER	Redacted S(9)2a Head of Privacy Governance Group
DATE APPROVED	[REDACTED] 29 August 2018
APPROVER	ACC Board
DATE OF REVIEW	29 August 2020

1 Policy Statement

ACC's Privacy Policy sets out the standards that support the way we use personal and health information in our care. We are committed to managing information as carefully and respectfully as if it were our own.

We are focused on being a leader of privacy practice in New Zealand. This means we have a strong privacy culture in the workplace, which focuses on protecting and appropriately managing personal information. We look for opportunities to improve systems and processes to manage risk and integrate the principles of privacy by design throughout ACC.

2 Objective

This policy aims to promote high standards for managing personal and health information and to ensure compliance with the Privacy Act 1993 and the Health Information Privacy Code 1994. It is a vehicle for guiding and training staff, and providing assurance that all employees understand their responsibilities.

3 Scope

All our people, including our Board members, contractors and third parties (to the extent of our influence), must comply with this policy.

This policy applies to all personal information, defined as information about an identifiable individual. This includes physical and electronic documents and can include information held in the mind of ACC's employees, if that information is readily retrievable.

We are also a health agency that manages health information, which is information about an individual's medical history, disability or health services provided to an individual.

4 Policy Principles and Standards

The Privacy Policy is underpinned by the principles and rules of the Privacy Act 1993 and Health Information Privacy Code 1994. These govern how agencies manage personal and health information throughout the information lifecycle: collection, use, storage, access, correction, use and disclosure.

4.1 We carefully manage the collection of personal and health information. We collect personal and health information for purposes linked to our organisational purpose. We can only collect the information necessary to carry out our functions and responsibilities.

4.2 Our information is collected primarily from individuals who make an injury-related claim or pay levies. Staff who gather information for ACC are guided by internal procedures and training that specifies the boundaries of collection. These procedures guide instances when information needs to be obtained from indirect sources such as staff, medical providers, employers, government agencies, or to fulfil our health and safety obligations.

4.3 We commit to making people aware of the collection of information. We will inform them of our purpose for collection and their rights to access and correct that information. Irrelevant and unnecessary information will be returned to the supplier or destroyed where practicable.

4.4 We facilitate access to personal and health information as a key priority. We commit to providing individuals with access to their personal and health information, unless an exception under the legislation applies. Requesters are verified and the information is provided to them within legislative timeframes and boundaries.

4.5 We respect the individual's right to seek amendment of factually incorrect information. Our people follow process regarding the facilitation of such requests and where information is unable to be corrected. They will invite the individual to submit a statement of correction and ensure that it is read together with the original document in future.

4.6 Information held by us will be used and disclosed according to legislation.

We use information to:

- Assess entitlements to compensation, rehabilitation and medical treatment.
- Assist the evaluation of our services and performance.
- Contribute to research into injury prevention and effective rehabilitation.
- Ascertain levy payments and maintain the Scheme.

Personal and health information is used and disclosed for the purposes consistent with the reason it was obtained, and the core business purposes of ACC. Reasonable steps will be taken to ensure personal and health information is complete, relevant and up to date.

4.7 Personal and health information is disclosed to other parties only where there is legal authority to do so. We may use and disclose personal and health information to fulfil our legislative obligations and protect the health and safety of staff and third parties. We will take reasonable steps to ensure third parties protect the personal and health information we share with them in line with legislation and with the same care we give to it.

4.8 We commit to storing information with reasonable safeguards against loss and disclosure.

Reasonable safeguards include using physical and technological protections against unauthorised access. We will not keep information for longer than is necessary or allowed by legislation.

4.9 We have a clear, consistent processes for reporting, managing and escalating privacy incidents. Privacy incidents reported within ACC include breaches, near misses, or loss of our client data caused by parties contracted to us. Incidents will be resolved at the source as soon as practicable and affected parties are notified as appropriate. Breaches will be reported externally according to the standards set by the Government Chief Privacy Officer and legislation.

4.10 We will train our employees and contractors in personal and health information management. New staff are trained to ensure the privacy principles are applied when fulfilling their role within ACC. Existing staff are required to undertake regular training on privacy risk areas specific to their business area, as well as broader privacy principles.

4.11 We will protect the privacy of staff members. Staff's personal and health information is treated with the utmost care and respect, in accordance with legislative privacy requirements.

4.12 We commit to retaining up to date privacy processes. Our business processes relating to the collection, recording, access, use, storage and destruction of personal and health information will be regularly reviewed to ensure they reflect our privacy strategic intention and remain relevant and accessible to staff. We take a continuous improvement approach, and look for opportunities to adopt best practice from domestic and international experience.

4.13 We will use privacy by design in change initiatives. We proactively embed privacy into the design and operation of IT systems, networked infrastructure, and business practices. Privacy measures are not add-ons, but fully integrated components of the system.

5 Accountabilities

Board responsibility for privacy and information management is set out in our Board Governance Manual. This acknowledges that the Board is committed to managing personal and health information by:

- Setting clear expectations regarding privacy and protection of personal and health information, and communicating them to the executive management.
- Holding executive management accountable for meeting those expectations.
- Ensuring that effective privacy risk management is fully embedded within our overall risk management activities.
- Implement high-quality monitoring and information management practices.

To support the Board, our managers are directly accountable for identifying and addressing privacy risk in their own units and reporting incidents to the Board via the Chief Governance Officer.

The Chief Governance Officer, on behalf of the Executive, is accountable for ensuring that supporting guidelines, operational measures and monitoring are in place.

6 Responsibilities

Role	Responsibilities
Employees, including contractors, consultants and temporary staff engaged by ACC	All ACC employees have individual responsibility to maintain best privacy practice behaviours, report all privacy breaches and near misses to a manager, promote privacy at work, comply with privacy policies, actively participate in privacy training and identify privacy risks.
People Managers	<p>People Managers have specific responsibilities for:</p> <ul style="list-style-type: none"> • Notifying privacy incidents to their manager. • Proactively assessing and managing privacy risk. • Managing all privacy reporting requirements through the Privacy Reporting Tool. • Liaising with the Talent Group following all privacy incidents to ensure consistent follow up with staff. • Owning the unit's Privacy Risk Register and ensuring it is kept current. • Ensuring staff are aware of and recognise the importance of their role in privacy. • Ensuring staff are aware of and compliant with our Privacy Policy, the Privacy Act 1993, the Health Information Privacy Code 1994, and complete their annual privacy training. • Ensuring new staff induction includes privacy training.
Privacy Officer	The Privacy Officer supports compliance with this policy and the relevant legislation. The Privacy Officer oversees investigations into privacy-related complaints lodged with the Privacy Commissioner and ACC.
Head of Privacy	The Head of Privacy supports compliance with this policy and the relevant legislation. They are also responsible for the management of the privacy function including breach and complaint management, measuring and reporting on our privacy performance, setting our privacy strategy, implementation of our privacy maturity plan, privacy risk identification and mitigation and privacy stakeholder engagement.
Chief Governance Officer	<p>The Chief Governance Officer:</p> <ul style="list-style-type: none"> • Is responsible for ensuring that organisational controls are in place to support and raise awareness of this policy; report and analyse privacy incidents to identify root causes of privacy incidents; and develop training to disperse privacy knowledge throughout ACC • Represents the Executive team in relation to all matters regarding privacy.
Executive	Executive will model best privacy practices and ensure privacy is core to all aspects of our culture.
Board	Board is responsible for ensuring the organisation is aware of the need to look after our customers' information through high-quality monitoring and information management practices.

7 Monitoring and oversight

Our privacy policies and guidelines have been established to comply with the Privacy Act 1993 and Health Information Privacy Code 1994.

The monitoring and oversight of privacy follows the five lines of assurance model to provide assurance that staff and third party privacy risks are being managed effectively under different situations.

Line of Assurance	Responsibility
<p>1st Line</p> <p>Employees</p> <p>People Managers</p>	<ul style="list-style-type: none"> • Our people are responsible for recognising and proactively managing privacy risks. • First line activities include: <ul style="list-style-type: none"> ○ Embedding privacy responsibilities in the business ○ ensuring Privacy-by-Design is embedded into new business design ○ regular privacy training and updates ○ monitoring and reporting ○ Clear guidelines for business as usual processes ○ Breach reporting
<p>2nd line</p> <p>Privacy Team</p>	<ul style="list-style-type: none"> • Our second line functions are to support the business in the management of privacy risk. • Second line activities include: <ul style="list-style-type: none"> ○ Monthly reporting on our privacy breaches and Enterprise Risk Reporting to the Executive and Board ○ Attestation compliance ○ Delivery of the privacy programme ○ Root cause analysis of breaches ○ Privacy assurance reviews ○ Ownership of privacy policies and guidelines ○ Specialist advice and support, including privacy-by-design
<p>3rd line</p> <p>Assurance Services</p>	<ul style="list-style-type: none"> • Third line functions provide independent information on the overall reliability of processes and performance. • Third line activities include: <ul style="list-style-type: none"> ○ Assurance Services schedule of continuous assurance activities for privacy. ○ Annual privacy self-assessment commissioned by

<p>Office of the Privacy Commissioner</p>	<p>Government Chief Privacy Officer to test our privacy maturity.</p> <ul style="list-style-type: none"> ○ Annual audit of privacy measures. <p>The Office of the Privacy Commissioner provides external monitoring and oversight of our compliance with the Privacy Act through its advice and complaints functions, and public reporting on these.</p>
<p>4th line Executive</p>	<ul style="list-style-type: none"> • Our Executive has overall responsibility for building and maintaining robust privacy risk management processes and received regular reports on: <ul style="list-style-type: none"> ○ Privacy as an Enterprise Risk ○ Privacy compliance ○ Progress against the Privacy Maturity Assessment Framework.
<p>5th line Board</p>	<ul style="list-style-type: none"> • Our Board has overall responsibility for ensuring that privacy risk management is in place and are responsible for setting the Privacy Risk Appetite Statement. The Board received regular reports on: <ul style="list-style-type: none"> ○ Privacy as an Enterprise Risk ○ Privacy compliance ○ Progress against the Privacy Maturity Assessment Framework.

8 Breaches of Policy

Complying with all policies and procedures is an expectation outlined in the Code of Conduct. Behaviours, 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.

9 Contacts

Questions regarding the interpretation or management of the policy can be directed to the advisors in the [Privacy Team](#).

10 Definitions

- **Privacy Maturity Plan** – Formalises our approach to improving privacy maturity between 2016 and 2020. It embeds a culture of information stewardship that aligns with the other being made to improve our customers' experiences.
- **Privacy by design** – A design approach where privacy is engineered into the design and architecture of information systems, business processes and networked infrastructure.

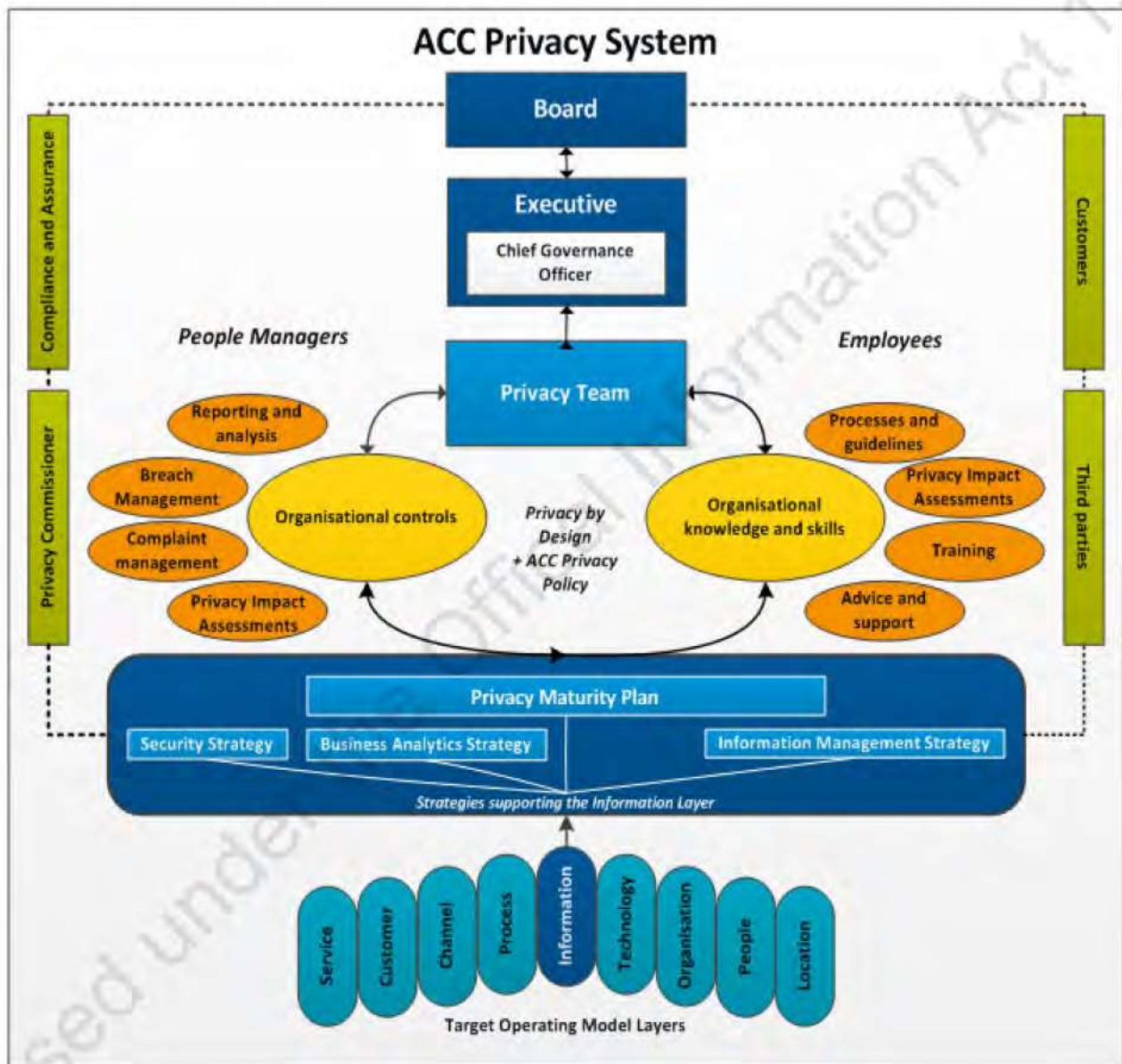
11 References

This policy should be read in conjunction with the [Privacy Maturity Plan](#), as well as the [Information](#)

Appendix 1: Policy System Diagram

Privacy is one of our strategic intentions and there is accountability for privacy throughout the organisation, from the Board and Executive to managers and employees.

An overview of our Information Management Framework is detailed in the diagram below. It shows how key aspects work together to achieve strategic objectives for privacy as delivered through this policy.



Appendix 2: Processes and policies supporting the Privacy Policy

OVERARCHING DOCUMENTS	
ACC Board Governance	Board Responsibility for privacy

Manual	
ACC Privacy Maturity Plan	Four-year strategy for improving ACC's privacy maturity
POLICIES (Level 1)	SUPPORTING PROCEDURES & GUIDELINES:
<p>Information Management Policy</p> <p>The Information Management Policy sets out the standards that support the development, delivery, monitoring and review of ACC's Information Management practices.</p>	ACC's Information Management framework
POLICIES (Level 2)	SUPPORTING PROCEDURES & GUIDELINES:
<p>Privacy Policy</p> <p>Sets out the principles used by ACC to collect, use, disclose and store personal and health related information. It forms the basis of how ACC will handle, process, manage and destroy private personal and health information.</p>	<p>Intranet CHIPs guidelines:</p> <ul style="list-style-type: none"> - Summary of Information Privacy Principles Brief description of the Information Privacy Principles from the Privacy Act 1993 - Summary of Health Information Privacy Code Brief description of the Health Information Privacy Rules from the Health Information Privacy Code 1994 - Differences between personal and health information Explanation of how personal and health information differ, and what staff should know - Complete information privacy principles Full detail of the Information Privacy Principles from the Privacy Act 1993 - Complete health information privacy rules Full detail of the Health Information Privacy Rules from the Health Information Privacy Code 1994 - Privacy breaches Description of privacy breaches to aid in the management of a breach - Managing privacy breaches Process for reporting a privacy breach or near miss and escalating it to manager so they can determine how to address the situation and reduce the risk of it happening again - Privacy breach details checklist Checklist of questions to ask someone who informs ACC that they have received someone else's information - Privacy breach and near miss examples Examples of privacy breaches and near misses to use as a guide when managing a privacy breach
Privacy Policy (continued)	<p>Privacy of staff information policy</p> <p>Description of how ACC uses, retains, discloses and disposes of personal information held about its staff and applicants who are part of the staff recruitment process</p>
	<p>Offsite document security policy</p> <p>Relating to the care of physical documentation in the custody of ACC staff outside ACC premises (excluding electronic media)</p>
	<p>Approved Information Sharing Agreements</p> <p>A guide to the process of establishing and key requirements for setting up an AISA</p>
	<p>Access</p> <p>Outlines the principles for access to information, the legislative framework, requirements</p>

Privacy Policy (continued)	<p>around information requests and key points for responding to requests</p> <ul style="list-style-type: none">- Personal information requests Rules about requests for personal information, full client copy files, call recordings, and how to deal with multiple client references in one email- Withholding personal information Explanation around why staff might need to withhold personal information when requested by the client or their representative or guardian- Legal privilege or advice Principles and rules around legal professional privilege, privileged information disclosure, information requests, legal opinions and witness summons- Responding to request for information Process for responding to information request from a client, advocate or external party- Examples of declining personal information requests Reasons and examples of when we may decline a personal information request- Preparing client information in a CIT The process for Client Information staff when preparing a copy of a client's file in response to a request for personal information, or for a review or appeal hearing- Dispatching information prepared by CIT The process for Client Information staff to use to dispatch information prepared for a client's personal information request- How to do an EmailXtender search in Outlook (CIT) Instructions for Client Information staff on how to do an EmailXtender search in Outlook when they need to run a query in response to a request for client emails- Request for access log/footprint report Rules for responding to a request for a log of staff access to a client file in Eos
	<p>Accuracy</p> <p>Guidelines to ensure the information held about clients and customers is accurate</p> <ul style="list-style-type: none">- Verifying client's email using Email Toolset Process to verify new client email addresses, or to re-verify existing email addresses that have not been checked for 12 months or more- Verifying employer contact email using Email Toolset Process to verify new email addresses for employer contacts, or to re-verify existing email addresses that have not been checked for 12 months or more- High profile clients Rules for managing high profile clients in terms of confidentiality and file access- Managing high profile client claims Criteria to identify and process high profile client claims- Recording date of death The process to make sure the Eos party record is updated so no further correspondence will be sent to a client who is deceased- Client identity Rules to verify a client's identity to deal with the right person and prevent fraud- Gaining client authority Process for gaining client authority to collect relevant information from external parties- Verifying client ID Requirements to obtain and verify a client's identity

Privacy Policy (continued)	<p>Collection</p> <p>Outlines the collection principles including the purpose of collection, source of information and collection of information from the individual</p> <ul style="list-style-type: none">- Advocates and holders of authority to act Rules around ACC's process for obtaining third party authority to act on a client's behalf- Recording authority to act Instructions for actioning a client request to give someone authority to act on their behalf for all currently managed claims- Recording meetings Guidance for managing client requests to record meetings- Clients opting out of research Guidance for actioning client requests to opt out of research and preventing future contact- Authority principles Tips on the best way to obtain authority from clients to collect their information
	<p>Correction</p> <p>ACC's obligations when correcting client and customer information</p> <ul style="list-style-type: none">- Managing a client's request to change personal information Process for Case Owners to follow when they receive a request to change personal information held by ACC
	<p>Disclosure</p> <p>Guidance and principles around disclosing client information</p> <ul style="list-style-type: none">- Guidelines for information disclosure and requests Information on handling information requests, withholding information, and disclosing information to protect a client's privacy or legal professional privilege- Privacy check before disclosing information Rules around privacy checking client information, enclosure types, addresses, delivery options for sending information, and what to do when client information is returned- Limits on using and disclosing information Sets out how ACC can use and disclose client information that is collected- Disclosure of clients' health information to employers Rules around what client health information ACC can disclose to employers- What to say in a voicemail message Guidance around what information may or may not be left in a voicemail message- Interagency reporting Protocols for reporting at-risk clients and children or any suspicious activity to another Government agency- Client information requests from insurers Rules and requirements around handling client information requests from insurers- Disclosing information (process) Rules and processes for the various methods of disclosing information- Processing requests for pre-employment checks Process for staff to follow upon receipt of a request for a pre-employment check- Reporting crime activity Rules for disclosing information to third parties about suspected criminal activity- Disclosing information technical reference Process for staff to use when sending any information to an external party by email, post,

	<p>courier or fax</p> <ul style="list-style-type: none">- UK DSS requests <p>Process for Claims Management staff to use when arranging a medical report for the Department of Social Security (DSS) beneficiary</p> <ul style="list-style-type: none">- Advocate communications <p>Rules and guidelines for communicating with advocates about their clients</p>
	<p>Retention</p> <p>Outlines the retention periods for personal information as guided by ACC's Records Management Policy</p>
	<p>Storage and security</p> <p>Provides guidance to help staff store information safely</p> <ul style="list-style-type: none">- Preparing and sending a courier package <p>Process for sending a package by courier and ensuring the most appropriate courier method is used for the customer</p> <ul style="list-style-type: none">- Courier options available at ACC <p>Description of the courier options available when sending a package</p> <ul style="list-style-type: none">- Sending confidential information by courier using pre-alert <p>Process for ACC staff to follow to guarantee a signature is obtained from the correct recipient when sending confidential or sensitive information by courier</p> <ul style="list-style-type: none">- FAQs about delivering personal information <p>A reference for talking to clients about delivery of their personal information</p> <ul style="list-style-type: none">- FAQs about releasing information to employers <p>Guidelines for the type of information that can be released to employers about a work-related injury claim</p> <ul style="list-style-type: none">- Email <p>Series of policies regarding checking outgoing email, email content, and when emails should be sent</p> <ul style="list-style-type: none">- Checking address returned mail <p>Process to confirm the client's correct address details when a letter is returned</p> <ul style="list-style-type: none">- Sending information by fax <p>Process for sending information by fax to an external party (if fax is the only communication method available)</p>
	<p>Unique identifiers</p> <p>Guidelines and key points about unique identifier numbers, and information about the National Health Index number</p>
	<p>Use</p> <p>Guidelines and exceptions for the use of personal and health information</p> <ul style="list-style-type: none">- Limits on using and disclosing personal information <p>Rules about ACC use of information, or releasing information outside of ACC</p>
ADDITIONAL DOCUMENTS	
	<p>Cloud computing policy</p> <p>Policy to define the principles for ensuring that cloud computing solutions are assessed, adopted and managed in accordance with ACC's business needs and legislative obligations</p>
	<p>Code of Claimants' Rights</p>

Rules and purpose of the Code of Claimants' Rights

[Records Management Policy](#)

Policy to ensure that ACC staff and customers have confidence in the integrity of the information, and can effectively share and work collaboratively with information while complying with relevant policies and legislation, reducing the risk to ACC

Released under the Official Information Act 1982

Procurement Policy



POLICY NUMBER	4.2.0
TOPIC	Procurement Policy (level 2 policy)
OWNER	[REDACTED] Head of Procurement Procurement Services Finance
DATE APPROVED	10 October 2018 – effective from 1 November 2018
APPROVER	John Healy (Chief Financial Officer)
DATE OF REVIEW	10 October 2020

1 Policy Statement

This policy outlines our position when undertaking purchasing and procurement activities.

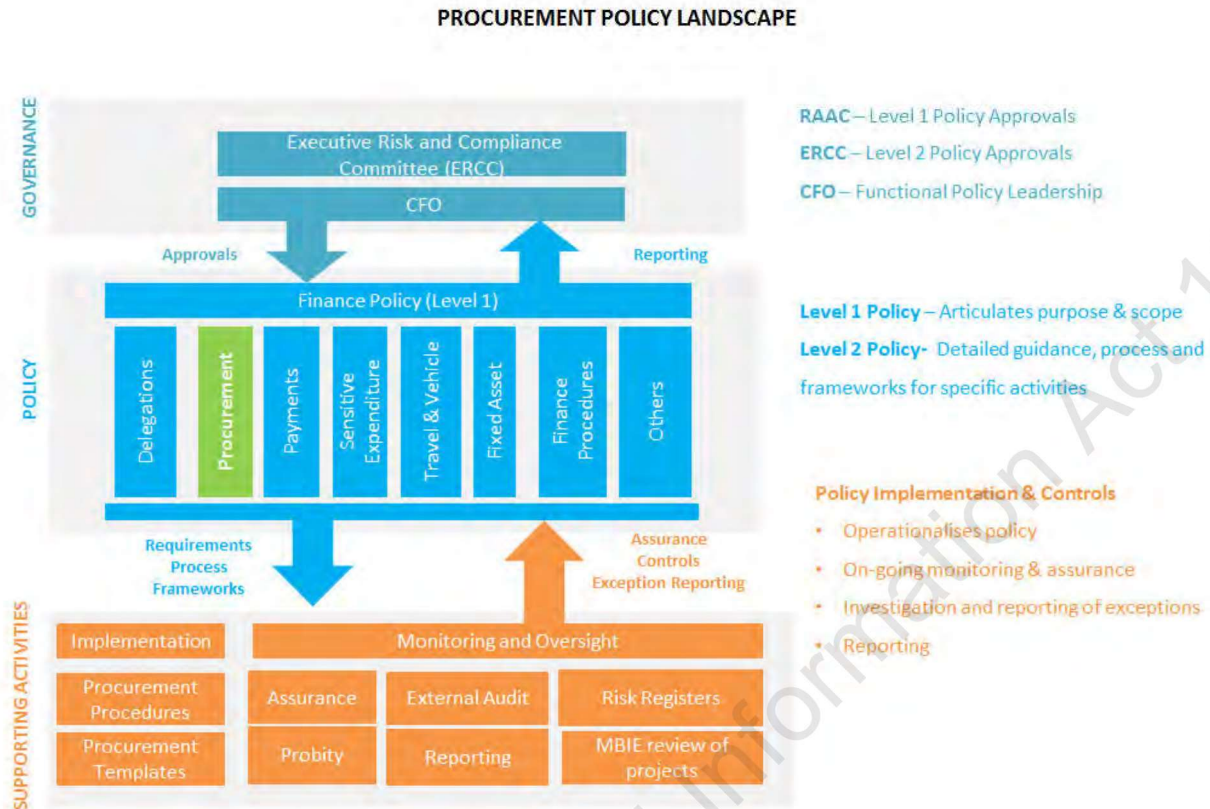
2 Objective

The objective of this policy is to ensure that procurement activity at ACC is fair, transparent, effective and consistent with the **Government Rules of Sourcing** and achieves good outcomes for ACC and our clients.

3 Scope

This policy applies to our people who are involved in purchasing or approving the purchase of goods or services on behalf of ACC, or managing contracts or relationships with suppliers.

4 Policy System Diagram



5 Policy standards

5.1 Government requirements are incorporated into any procurement activity
As a Crown entity, we must comply with the [Government Rules of Sourcing](#).

All-of-Government, Common Capability and Syndicated Contracts

5.2 We must purchase from the All-of-Government Contracts
We must purchase from the All-of-Government Contracts unless there is a good reason not to ([Rule 55](#)). If ACC wants to opt-out of purchasing from an All-of-Government Contract, employees must consult with the Head of Procurement and obtain approval from the Chief Executive (via the relevant Tier 2 Chief) and the relevant Functional Leader (the Department of Internal Affairs for ICT, the MBIE / Government Property Group for property, and MBIE for procurement).

5.3 We must purchase from mandatory Common Capability Contracts
We must purchase from mandatory Common Capability Contracts where the contract reasonably meets ACC's needs ([Rule 57](#)). If ACC wants to opt-out of purchasing from a mandatory Common Capability Contract, employees must consult with the Head of Procurement and obtain approval from the Chief Executive (via the relevant Tier 2 Chief) and the relevant Functional Leader or the lead agency managing the contract. We should participate in non-mandatory Common Capability Contracts before approaching the market for the same or substantially similar goods or services.

5.4 We should purchase from Syndicated Contracts
We should participate in Syndicated Contracts before approaching the market for the same or substantially similar goods or services ([Rule 56](#))

General

5.5 We will plan and manage procurement activities

We plan and manage procurement activities to realise the best outcomes. This includes involving suppliers early, taking the time to understand the market and our effect on it and choosing a process proportionate to the size, complexity and risk of the procurement.

5.6 We will be fair to all suppliers

We treat all suppliers equally and do not discriminate against any suppliers. We will make it easy for suppliers to do business with us. We will clearly explain how we will assess their proposals, and communicate with them so they know how to improve next time.

5.7 We will engage the appropriate supplier for our needs

We procure goods or services from the supplier who can deliver what we need, at a fair price, and on time. We will be clear about what we need and fair in how we assess the suppliers.

5.8 We will achieve the best result for everyone

We engage suppliers that deliver the best value for money considering the social, environmental and economic effects of the purchase and can account for all costs and benefits over the lifetime of the goods or services.

5.9 We will be good partners

We work together with suppliers to ensure, so far as reasonably practicable, that the work being done for, or on behalf of, ACC is healthy and safe as described in our [Health and Safety Policy](#). This includes the health and safety of people on our premises and wherever the work is taking place.

5.10 We will make procurement decisions according to approved delegations

All procurement decisions must be approved in accordance with the corporate delegations such as procurement plans, go to market activity, selecting suppliers (including direct sourcing and closed competitive), approving contracts and variations to contract.

5.11 We will act lawfully and responsibly

Our actions in procuring goods or services follow the relevant legislation and Government Rules of Sourcing rules and principles. ACC Personnel will be accountable for their actions and our process will be fair, transparent, and reasonable.

5.12 We will declare our conflicts of interest

We must declare any actual, perceived, or potential conflicts of interest in accordance with the [Conflicts of Interest Policy](#). We will manage the conflict of interest in line with our procurement manual. We must ensure adequate separation of responsibilities to avoid bias, or the perception of bias in relation to procurement decisions.

5.13 We must act with integrity

We must ensure that our actions throughout the procurement process are impartial and can withstand scrutiny from internal and external parties (for example, they must comply with the Code of Conduct).

5.14 We will only accept gifts in limited circumstances

We must only accept gifts and hospitality from a supplier in accordance with the Gifts and Gratuities Policy. We must never accept gifts or hospitality from a supplier who is participating in a current ACC procurement process. A procurement process is not complete until a contract has been executed, or the procurement has been cancelled.

5.15 We will keep and manage our documentation

We must retain all documents concerning any stage of a procurement process (including approval, go-to-market and the responses, evaluation, contract and variation documents), in accordance with

the [Privacy Policy](#) and file and archive in accordance with the [Records Management Policy](#) and Rules 49 and 50 of the [Government Rules of Sourcing](#).

6 Accountabilities

The Head of Procurement has overall responsibility and accountability for the operation of this policy. In addition:

- the Manager Health Procurement & Contracting has responsibility and accountability for the operation of this policy concerning health-related procurement; and
- the Strategic Partner Manager has responsibility and accountability for the operation of this policy concerning IT-related procurement.

7 Responsibilities

ACC has the following roles and responsibilities embedded in the organisation:

Role	Responsibilities
All employees	We all have individual responsibility to comply with the Procurement Policy and Procedures Manual, and Corporate Delegations and to engage with Procurement and Legal in a timely manner when required. We are responsible for complying with the Procurement Manual and Government Rules of Sourcing as well as ensuring approvals for procurement decisions are made in accordance with the Corporate Delegations.
Cost Centre Managers	Our cost centre managers are responsible for operating within their budget and ensuring that budget has been approved, and engaging Procurement in a timely manner where required
Contract Managers / Relationship Owners	Primary person who has overall management of the relationship and the performance of the supplier in line with the original engagement / contract.
Procurement Team	Procurement teams are responsible for following good procurement practice, and educating the business on good procurement and commercial practices and work collaboratively across Government when required
Manager Business Improvement & Support	Responsible for keeping this policy current
Strategic Partner Manager	Responsible for the operation of this policy concerning IT-related procurement
Manager Health Procurement & Contracting	Responsible for the operation of this policy concerning health-related procurement
Head of Procurement	Head of Procurement is the functional lead for procurement and commercial activities for ACC; represents ACC across Government and has overall responsibility for the operation of this policy
Chief Financial Officer	Chief Financial Officer is responsible for ensuring that organisational controls are in place to support and raise awareness of this policy

Executive	The Executive ensures good procurement practices, ensure compliance with the Government Rules of Sourcing, and ACC procurement policy, the corporate delegations and the procurement procedures
Board	The Board is responsible for approving Procurements in line with the corporate delegations

8 Monitoring and oversight

Line of Assurance	Monitoring and oversight activities:
1st line Our people People managers/ cost centre managers Relationship managers / contract managers	<ul style="list-style-type: none"> Ensure that procurement activities are carried out in accordance with the Government Rules of Sourcing, Procurement policy, and Procedures Manual. The Procurement newsletter and training are provided to the business to inform and educate on best practice procurement activities and process Ensure that any conflicts of interest are declared in a timely manner and managed appropriately Comply with the corporate and claims management delegations Cost centre manager will work within their allocated budgets, ensuring that the budget has been agreed, and will engage Procurement in a timely manner where required. Relationship managers / contract managers monitor and manage the supplier in line with the Provider Management Framework ensuring they deliver the services or products according to planned outcomes along with the monitoring and managing the expenditure
2nd line Procurement teams	<ul style="list-style-type: none"> Update and maintain risk registers to capture risk arising from compliance with Government Rules of Sourcing, capability, capacity and legislative compliance Review procurement procedures and templates that are used by procurement, and provided, and used by the business for low value procurement. Ensure Government Rules of Sourcing exemptions and opt-outs are reviewed and approved by the relevant delegated authority and are recorded in a central register. Obtain approval and report on non-compliant procurement exemptions and opt-outs Monitor compliance with the Procurement policy and procedures Store declared conflict of interests and management plans in the procurement central folder. Respond to Ministry of Business, Innovation and Employment (MBIE) requests within their timeframes. Periodic review and consultation with MBIE on procurement projects including reporting of annual procurement plan, significant services contracts and procurement capability index. MBIE assess our procurement projects when >\$5M Provide the Procurement dashboard to Executive.

	<ul style="list-style-type: none"> The Provider Service Delivery governance model and steering committee will approve all health procurement projects. The Chief Technology Officer and Head of Partnerships approve all IT procurement projects Internal and external probity is considered for procurement projects and assessed according to the guidelines
3rd line Assurance Services External audits	<ul style="list-style-type: none"> Assurance Services independently audit procurement policy and procedures and activity. Independent external auditors appointed on behalf of the Office of the Auditor General provide assurance on procurement policy and procedures.
4th Line Executive	<ul style="list-style-type: none"> The Executive and Head's of approve procurement projects in line with the Corporate Delegations The Chief Executive and Chiefs have primary responsibility for our strategic objectives and reporting to the Board on the management of these objectives.
5th line Board	<ul style="list-style-type: none"> The Board approve procurement projects in line with the Corporate Delegations. The Board has overall responsibility for ensuring effective risk management is in place. Reviews and assesses the Chief Executive's and Chiefs reporting and management of objectives.

9 Breaches of Policy

The Code of Conduct requires all employees to comply with all policies and procedures. Behaviour or actions that are investigated and found to be in breach of the Code of Conduct may result in disciplinary action.

The rationale for any non-compliance of the [Government Rules of Sourcing](#) must be documented, and made available to MBIE if requested.

10 Contacts

For issues of interpretation or management of this policy or updates you should contact:

- [Health Procurement](#) for health-related procurement
- [IT & A Business Enablement](#) for IT-related procurement
- [Procurement Services](#) for all other procurement matters.

11 Definitions

All-of-Government Contract	A type of approved collaborative contract. Supply agreements are established with approved suppliers for selected common goods or services purchased across government. They are developed under the oversight of the Procurement Functional Leader (Chief Executive of MBIE) and managed by appointed procurement Centres of Expertise.
----------------------------	--

Closed Competitive process	Also known as selective procurement, this is where ACC invites a limited number of known suppliers to respond to a contract opportunity (and the contract opportunity is not openly advertised).
Common Capability Contract	A type of approved collaborative contract. Various supply agreements are established with approved suppliers for selected common goods or services or works purchased across government.
Direct Source process	Also known as direct procurement, this is where ACC contracts directly with a selected supplier/s for the required goods or services
Government Rules of Sourcing (Rules)	The Rules represent the government's standards of good practice for procurement planning, approaching the market and contracting Cabinet has endorsed the Rules (CAB Min (13) 10/4A) and they came into effect on 1 October 2013. The Rules replaced the 2006 Mandatory Rules for Procurement by Departments The Rules became mandated for ACC on 1 February 2015.
MBIE	The Ministry of Business, Innovation and Employment.
Syndicated Contract	A type of approved collaborative contract. They typically involve a cluster of agencies aggregating their respective needs and collectively going to market for common goods or services. It may also involve an agency or agencies anticipating collaboration and including a Common Use Provision (CUP) clause within the resulting contract, which allows other agencies to contract with the supplier on the same terms later
Tender	A process to seek responses from the market regarding the purchase of goods or services, such as a Request for Proposal, Request for Tender or Request for Quote. See the Procurement Manual for more information.

12 References

This policy is supported by, and must be read in conjunction with, the Delegations Manual, ACC's Procurement Manual and ACC's Procurement Method Guidelines. In the event of any inconsistency, the following hierarchy of precedence will apply:

- The [Government Rules of Sourcing](#)
- [The Delegations Manual](#)
- This policy
- [The Procurement Method Guidelines](#)
- [The Procurement Manual](#)



Leave Policy

POLICY NUMBER 2.6.0

TOPIC Leave Policy

OWNER [Redacted] Management Relations Talent Group

DATE APPROVED March 2019 [Redacted]

APPROVER Sharon Champness
Chief Talent Officer

DATE OF REVIEW March 2021

1 Policy Statement

ACC aims to promote a safe and healthy work life balance, to promote wellbeing and performance within the organisation. Taking leave and having leave available for unplanned situations is one way in which ACC can achieve this.

2 Objective Scope

The purpose of the Leave policy and procedures is to ensure everyone working at ACC has the information and guidance needed when applying or approving leave.

3 Scope

This policy applies to all ACC employees.

The provisions relating to individual leave entitlements are set out in employment agreements and letters of offer.

4 Policy statements

4.1 ACC recognises the following types of leave:

Planned leave	Unplanned leave
<ul style="list-style-type: none">Annual Leave including Anticipated Annual LeaveLeave without payLong service leaveParental leaveStudy LeaveTime off in Lieu	<ul style="list-style-type: none">Sick leaveDomestic leaveBereavement leaveAccident leaveAttendance at emergency operations

<ul style="list-style-type: none">• Alternative Public Holiday• Special representatives leave• Jury service leave• Witness leave• Military leave• Team Volunteering Leave• Union Meetings• Employment Relations Education Leave	<ul style="list-style-type: none">• Domestic Violence leave• Paid Special Leave
--	--

4.2 Employees are expected to give reasonable notice when applying for leave.

For planned leave, four weeks is considered reasonable.

ACC recognises unforeseen circumstances may require leave requests to be submitted at short notice. Although leave approval will not be unreasonably denied, business needs/requirements will be considered when reaching an agreement about the timing and length of leave.

For unplanned leave,

- employees are expected to make reasonable efforts to contact their manager as soon as possible on their first day of absence; and
- maintain regular contact with their manager if they are absent for an extended period.

4.3 Leave requests will not be unreasonably denied

The intention is to act in good faith and balance individual and business needs. Managers and employees will work together to ensure there is a common understanding of what reasonable means.

4.4 Employees are expected to have at least one continuous break of planned leave of at least two weeks in each 12-month period. This may include public holidays.

Managers and employees will discuss and agree on plan for a continuous break of at least two weeks. Managers may, after discussion and with two weeks' notice, direct employees to take annual leave entitlement in accordance with the Holidays Act.

4.5 ACC may close down parts of the business, requiring employees to take leave in accordance with the Holidays Act. Two weeks' notice must be given for any closedown.

This may happen between Christmas and New Year, but can happen at any time. During closedown periods, Annual Leave, Anticipated Annual leave, or Leave Without Pay would be considered.

Where any additional closedowns are required, other than the annual closedown, managers must agree with employees on how these are treated and what leave or holidays arrangements will apply.

4.6 Any breach of trust by taking time off work dishonestly will be regarded as serious misconduct.

5 Accountabilities

The Chief Talent Officer, for ensuring organisational controls are in place to support this policy.

6 Responsibilities

Roles:	Responsibilities:
Employees	<ul style="list-style-type: none"> • Apply for leave through appropriate processes. • Give reasonable notice when applying for leave. • Notify your manager as soon as possible on the first day of an unplanned absence. • Work with your manager to create a leave plan annually.
People Managers	<ul style="list-style-type: none"> • Plan leave with employees. Leave plans should be completed annually. • Ensure all leave applications are considered fairly. • As a general rule, leave applications should be approved or declined within two days.
Talent	<ul style="list-style-type: none"> • Provide advice on relevant policies and procedures. • Maintain employee leave records and act on payment of approved leave. • Provide access for managers to information on leave accruals, entitlements and usage.

7 Monitoring and oversight

Lines of Assurance:	Monitoring & Oversight
1st line Employees People Managers	<ul style="list-style-type: none"> • Employees are expected to plan and manage their leave entitlements according to this policy. • Managers oversee employees use of leave and approve accordingly.
2nd line Talent Team	<ul style="list-style-type: none"> • Maintain employee record of leave entitlement and usage. • Manage HR help services to answer queries from employees or managers. • Monitor and update leave policies and procedures.
3rd line Assurance	<ul style="list-style-type: none"> • Independently assess appropriateness and adherence to this policy. • Assurance Services assess our compliance with legislative obligations in accordance with assurance plans approved by the Board.
4th line Chiefs	<ul style="list-style-type: none"> • The Chief Executive and Chiefs have primary responsibility for reporting to the appropriate governance committees and the Board on the management of our strategic objectives and monitoring the risks to achieving these objectives.
5th line	