IMCNZ Privacy and Information Security Policy

Institute of Management Consultants New Zealand (IMCNZ)

Document control	**Details**
Policy owner	IMCNZ Council
Accountable officer	IMCNZ President, on behalf of Council
Responsible officer	IMCNZ Privacy Officer
Privacy contact	privacy@imcnz.org.nz
Version	1.0
Approval authority	IMCNZ Council
Effective date	20 October 2026
Review frequency	Annually, or following a material incident or legislative change
Supersedes	IMCNZ Privacy Policy dated 30 August 2018

1. Purpose

The Institute of Management Consultants New Zealand (IMCNZ) is committed to protecting personal information, maintaining the confidentiality and integrity of Institute records, and ensuring that information entrusted to the Institute is managed responsibly.

This policy establishes IMCNZ's requirements for privacy protection, information security, appropriate information use, access management, record retention, incident reporting and accountability.

It is intended to ensure that IMCNZ:

- Meets its obligations under the Privacy Act 2020 and other applicable New Zealand legislation.
- Protects the personal information of members, applicants, stakeholders and other individuals.
- Maintains appropriate security over information systems, membership databases and confidential records.
- Prevents unauthorised access, disclosure, extraction, retention, alteration or misuse of Institute information.
- Establishes clear responsibilities for current and former Council officers, volunteers, contractors and service providers.
- Responds promptly and appropriately to privacy and information security incidents.
- Maintains the trust and confidence of members through transparent, consistent and accountable practices.

Privacy and information security are fundamental components of IMCNZ's professional governance responsibilities.

2. Scope and application

This policy applies to:

- All IMCNZ Council officers and Council members.
- All IMCNZ members when accessing or handling Institute information.
- Employees, volunteers, assessors, committee members and individuals appointed to undertake IMCNZ activities.
- Contractors, consultants, technology administrators and third-party service providers acting on behalf of IMCNZ.
- Former officers, members, contractors and service providers to the extent that they continue to possess, access or control IMCNZ information obtained through their roles.

It applies to information held or processed in any format, including electronic, physical, archived, cloud-based and third-party systems.

This includes membership records, financial information, governance correspondence, complaints and dispute records, certification and assessment information, meeting documents, email accounts, mailing lists and system access credentials.

Obligations relating to confidentiality, authorised use, information return and secure disposal continue following the conclusion of an individual's role or engagement.

The Privacy Act 2020 applies to IMCNZ and relevant privacy-related conduct independently of whether Council has an approved or published Privacy and Information Security Policy.

3. Policy principles

IMCNZ adopts the following principles:

Lawfulness: Information will be collected, used, disclosed and retained only for lawful and legitimate Institute purposes.

Purpose limitation: Information obtained for one purpose must not be used for an unrelated purpose unless authorised by law or otherwise permitted under the Privacy Act.

Confidentiality: Information will only be accessible to individuals with a legitimate, authorised need.

Accountability: Access to Institute information carries individual responsibility for its proper use and protection.

Transparency: Individuals will be informed about how their personal information is managed and how they may exercise their privacy rights.

Security: Reasonable technical, administrative and organisational safeguards will be applied proportionately to the sensitivity of information and associated risks.

Continuity: Institute information, accounts and records must remain under the effective control of IMCNZ regardless of changes in officeholders or service providers.

Independence: Privacy complaints and requests involving an officer with an actual or perceived conflict of interest will be managed through an appropriate alternative decision-maker.

4. Information collected and held

IMCNZ may collect and hold information necessary for its membership, governance, certification, professional development, administrative and statutory functions.

This may include:

4.1 Membership information

Names, contact details, organisation affiliations, membership categories, professional qualifications, employment or consultancy details, membership history, payment records and professional interests.

4.2 Certification and professional assessment

Applications, qualifications, professional experience, references, continuing professional development records, case studies, assessment outcomes and certification history.

4.3 Governance and administration

Council correspondence, meeting records (minutes), decisions (register), financial records, declarations of interest, appointment records and documents required for statutory or organisational accountability.

4.4 Complaints, disputes and professional conduct

Complaints, evidence, correspondence, investigation materials, findings, disciplinary decisions and related information necessary to administer IMCNZ's constitution, bylaws and dispute resolution procedures.

4.5 Website, events and communications

Event registrations, newsletter subscriptions, enquiries, website information and communications preferences. Technical information such as website usage data and cookies may also be collected where relevant and disclosed through appropriate notices.

IMCNZ will collect only information reasonably necessary for its lawful functions and will take reasonable steps to ensure individuals understand the purpose and intended use of that information.

Where personal information is collected indirectly, IMCNZ will comply with Information Privacy Principle 3A, including applicable notification requirements and exceptions.

5. Use and disclosure of personal information

IMCNZ may use personal information for:

- Administering membership and associated benefits.
- Managing certification, assessment and professional standards.
- Delivering events, professional development and member services.
- Communicating official Institute business.
- Meeting statutory, financial and governance obligations.
- Administering properly authorised complaints and dispute resolution processes.
- Protecting the Institute's legitimate operational and security interests.
- Other purposes permitted under the Privacy Act 2020.

Personal information must not be accessed, extracted, disclosed or used for purposes unrelated to authorised Institute activities without an appropriate lawful basis.

In particular:

1. Membership databases and contact lists must not be copied or exported for personal, commercial, political, campaigning or unrelated organisational purposes.
2. IMCNZ membership information must not be transferred to competing organisations, external mailing lists or private databases without appropriate authorisation and a lawful basis.
3. Individuals must not use access acquired through an IMCNZ role to conduct communications that falsely imply IMCNZ authorisation or endorsement.
4. Information obtained through confidential Council duties must not be disclosed or used outside authorised functions.
5. Confidential investigation or complaints information must not be circulated beyond individuals with a legitimate need to receive it.

IMCNZ may disclose information to regulators, law enforcement authorities, legal advisers, independent investigators, professional bodies and service providers where lawful and appropriate.

Information may be shared with the International Council of Management Consulting Institutes (ICMCI) where necessary for membership, certification, accreditation or other authorised professional activities, subject to applicable privacy requirements.

For the avoidance of doubt, the protections against unauthorised use or disclosure of personal information do not restrict lawful publication of member details, subject to member opt-out rights, in accordance with the IMCNZ Constitution.

6. Ownership, stewardship and custody of Institute information

All institutional records, documents, communications, databases and information created, received or maintained in the course of authorised IMCNZ activities are to be managed as records of the Institute, subject to applicable legal rights and obligations.

Access granted to an individual does not confer personal ownership or an unrestricted right to retain, reproduce, distribute or use Institute information.

Current and former Council officers and other authorised representatives must:

- Maintain Institute records in approved locations and systems.
- Make required records available to authorised successors.

- Preserve records subject to legal, regulatory, contractual or governance obligations.
- Return or securely transfer IMCNZ information when requested by authorised officers.
- Refrain from retaining unauthorised copies after their role concludes.
- Cooperate with reasonable information recovery, transfer and verification processes.

Where an individual asserts a legitimate legal basis for retaining particular records, the matter must be referred to the Privacy Officer or an independent authorised reviewer for determination.

Any return or deletion requirement must be consistent with applicable legal preservation obligations.

7. Information security requirements

IMCNZ will adopt a risk-based approach to information security, aligned with relevant guidance from the New Zealand National Cyber Security Centre.

7.1 Access control

Access to Institute systems and information must be approved and limited to the minimum permissions necessary for an individual's authorised responsibilities.

IMCNZ will:

- Maintain a register of information systems and authorised users.
- Allocate identifiable user accounts wherever practicable.
- Restrict administrator privileges to specifically authorised individuals.
- Review access when individuals change roles or leave the Institute.
- Periodically review privileged access and permissions.
- Maintain appropriate audit records of significant access activity.

Shared administrator credentials are prohibited unless there is a documented technical necessity, appropriate safeguards and Council-authorised oversight.

7.2 Authentication and system protection

Multifactor authentication must be enabled on supported systems containing Institute information, with priority given to email, website administration, membership systems, financial services and communications platforms.

Passwords must be strong, unique and securely managed.

Credentials must not be transmitted through insecure channels or retained in personal records accessible to unauthorised individuals.

Administrative recovery arrangements must remain under IMCNZ control, with appropriate separation of duties.

7.3 Information storage

IMCNZ information must be stored in approved, appropriately secured systems.

Sensitive information must not be routinely stored on personal devices, private email accounts, unmanaged cloud services or removable media.

Where authorised temporary use of such facilities is unavoidable, documented safeguards must be applied, including encryption, restricted access and timely secure transfer or deletion.

7.4 Member databases and communications platforms

Membership databases, including contact information held in email marketing and membership management platforms, are designated controlled information assets.

Exporting or bulk downloading membership records requires documented authorisation from an appropriate Council delegate and a legitimate business purpose.

Bulk exports must be recorded, including the purpose, approving person, recipient, location and disposal arrangements.

Platform permissions must prevent unauthorised exports wherever technical functionality permits.

Council will ensure that access to mailing platforms is individually attributable and periodically reviewed.

7.5 Monitoring and audit

IMCNZ may maintain and review system access logs, administrative records and relevant organisational communications for legitimate security, governance and compliance purposes.

Such activities must themselves comply with the Privacy Act, be proportionate and appropriately authorised.

Access to confidential or potentially privileged material for an investigation must be limited to those authorised to conduct that investigation, with legal advice obtained where necessary.

Any monitoring or examination of organisational communications must have appropriate authorisation, a proportionate scope and an auditable record of access.

7.6 Technology service providers

Technology and administrative service providers must be subject to appropriate due diligence and contractual controls addressing confidentiality, access, security, incident reporting, data return and termination arrangements.

Where information is stored or disclosed overseas, IMCNZ will assess its obligations under Information Privacy Principle 12 and implement necessary safeguards.

8. Council transitions, resignation and cessation of access

To protect organisational continuity and information security, all Council transitions and departures must be subject to a documented handover process.

8.1 Handover requirements

Departing officers and authorised representatives must, when reasonably directed:

- Return or transfer Institute correspondence and governance records.
- Surrender or transfer control of relevant accounts and administrative access.
- Identify any IMCNZ information held outside approved systems.
- Return physical documents, devices and other Institute property.
- Confirm the disposition of retained copies and backup information.
- Cooperate with verification of information completeness and accessibility.

Handover arrangements should normally be completed by the effective date of departure, with any outstanding actions documented and assigned a completion date.

8.2 Access termination

System access must be reviewed immediately upon notice of resignation, removal, role change or completion of engagement.

Access no longer required must be revoked promptly, with particular priority given to privileged accounts, databases, financial systems and communications platforms.

Where a material security risk exists, Council may authorise immediate suspension of access pending review, subject to applicable legal and constitutional requirements.

8.3 Failure to complete handover

Failure to comply with reasonable and lawful information return or handover requirements must be recorded and escalated to Council.

Where necessary and proportionate, Council may obtain legal advice, seek appropriate recovery measures, refer suspected unlawful conduct to competent authorities, or initiate procedures permitted under the Institute's governing instruments.

All such actions must be evidence-based, procedurally fair and consistent with applicable law.

9. Confidential Council information and disputes

Council officers, committee members, investigators, assessors and other authorised participants must maintain the confidentiality of information received through their official responsibilities.

Information relating to complaints, member disputes, disciplinary proceedings, privacy requests, internal investigations, legal advice or sensitive governance matters must be subject to heightened controls.

Access must be limited to individuals with an identified role in handling the relevant matter.

Council authorised investigators, subcommittees, decision-makers and reviewers must be given access to the complaint and investigation information reasonably necessary for their responsibilities under the Constitution and approved dispute-resolution procedures, subject to confidentiality, proportionality and applicable legal protections.

Individuals must not disclose confidential information to advance personal interests, undermine another individual, prejudice a properly constituted process or influence an investigation outside authorised procedures.

This provision does not prevent lawful whistleblowing, protected disclosures, reporting to regulators or law enforcement, exercising statutory rights, or obtaining independent legal advice.

Where there is an actual or reasonably perceived conflict of interest, the individual concerned must not exercise decision-making authority over the handling or disclosure of the relevant information.

10. Official communications and membership data

Official communications using IMCNZ's membership records must be issued through authorised Institute systems by approved individuals.

Council will establish and maintain controls to ensure:

- Member contact details are used only for legitimate and lawful purposes.
- Formal Council communications are appropriately authorised.

- Unsolicited or unauthorised bulk communications using membership information are prohibited.
- Recipients are given suitable communication preferences and unsubscribe arrangements where required.
- Marketing and promotional communications comply with the Unsolicited Electronic Messages Act 2007.
- Email distribution practices minimise unintended disclosure of recipient information.

Members must not infer that possession of IMCNZ contact information provides permission for unrelated communications.

Nothing in this section prevents Members from exercising their lawful rights under the Constitution, participating in Society governance, expressing opinions, raising concerns, making complaints or communicating through lawful means. These rights do not confer an entitlement to obtain, extract or misuse personal information held in IMCNZ systems.

Members may report suspected misuse of their information to privacy@imcnz.org.nz.

11. Privacy Officer and accountability

In accordance with section 201 of the Privacy Act 2020, IMCNZ will designate at least one Privacy Officer.

The Privacy Officer is responsible for:

- Supporting compliance with the Privacy Act.
- Facilitating access and correction requests.
- Advising Council on privacy obligations and risks.
- Coordinating privacy breach assessment and response.
- Managing the privacy incident and request registers.
- Promoting good privacy practices.
- Liaising with the Office of the Privacy Commissioner where appropriate.

The designated contact address is:

privacy@imcnz.org.nz

Privacy matters will be handled through a controlled mailbox with access restricted to the Privacy Officer and specifically authorised alternatives.

11.1 Independence and conflicts of interest

Where a privacy request, complaint or investigation concerns the Privacy Officer personally, or creates a material conflict of interest, the matter must be allocated to another appropriately authorised and independent individual.

Where Council involvement would create a conflict, Council should appoint a suitably independent external reviewer or adviser.

The individual subject to the conflict must not control substantive decisions about their own case, although they may be asked to provide relevant evidence.

Privacy requests must not be delayed solely because an internal conflict exists.

Council retains organisational accountability for compliance even where operational responsibilities are delegated.

Where a matter falls within the approved complaints and dispute-resolution framework, the Privacy Officer's administrative or compliance role does not displace the authority of duly appointed investigators, subcommittees or decisionmakers.

12. Access to and correction of personal information

Individuals have the right to request access to personal information IMCNZ holds about them and to request its correction, subject to the Privacy Act 2020.

Requests may be made through privacy@imcnz.org.nz or any other communication channel permitted by law.

IMCNZ will:

1. Record the date the request was received.
2. Acknowledge the request promptly.
3. Take reasonable steps to establish the requester's identity or authority before releasing personal information.
4. Identify and preserve potentially relevant records.
5. Assess applicable statutory withholding grounds and third-party privacy interests.
6. Make and communicate a decision as soon as reasonably practicable and no later than 20 working days, unless a lawful extension applies.
7. Provide approved information without undue delay.
8. Inform the requester of applicable rights to complain to the Office of the Privacy Commissioner.

Extensions will be considered only where permitted by law, notified within the statutory timeframe and accompanied by the required explanation.

Correction requests will be assessed in accordance with the Privacy Act. Where IMCNZ declines to amend information, applicable rights to attach a statement of correction will be respected.

Nothing in this policy limits a Member's right to request information under relevant clause of the IMCNZ Constitution or an individual's rights under the Privacy Act 2020. Requests will be assessed under the applicable legal and constitutional framework, recognising that different access rights, grounds for withholding and procedural requirements may apply.

13. Privacy breaches and information security incidents

A privacy or information security incident may include:

- Unauthorised access to personal information.
- Unauthorised export, copying or disclosure of membership data.
- Loss or theft of Institute records.
- Misuse of privileged access.
- Inappropriate retention or distribution of confidential information.
- Unauthorised use of member contact lists.
- Compromise of accounts, credentials or systems.
- Accidental disclosure of personal information.
- Unauthorised modification or destruction of Institute records.

13.1 Reporting

Any person who becomes aware of a suspected incident involving IMCNZ information must report it promptly to privacy@imcnz.org.nz or, where necessary, directly to an appropriate Council officer.

The report should include the nature of the incident, information potentially affected, relevant dates and any immediate containment action.

Individuals are not expected to establish conclusively that a breach occurred before making a report.

13.2 Incident response

The Privacy Officer, working with appropriately authorised Council officers and technical advisers, will coordinate the response.

This will include:

1. Recording and initially assessing the incident.
2. Containing any continuing exposure or unauthorised access.
3. Preserving relevant evidence and audit records.
4. Establishing the nature, scope and potential consequences.
5. Assessing whether individuals have suffered or are likely to suffer serious harm.
6. Determining applicable statutory notification obligations.
7. Coordinating any necessary regulator, law enforcement or affected-person notifications.
8. Implementing corrective actions and reviewing control weaknesses.

13.3 Notifiable privacy breaches

Where a breach has caused, or is likely to cause, serious harm, IMCNZ will notify the Office of the Privacy Commissioner and affected individuals as soon as practicable, in accordance with the Privacy Act 2020.

IMCNZ will aim to notify the Commissioner within 72 hours of determining that a breach is notifiable, consistent with the Commissioner's guidance.

Any decision to delay or withhold individual notification must have a lawful basis and be documented.

Where warranted, the incident may also be referred to New Zealand Police, the National Cyber Security Centre, affected service providers or other appropriate authorities.

13.4 Evidence preservation

Investigation evidence must be preserved securely, with access restricted and relevant handling recorded.

Records relevant to actual or reasonably anticipated investigations, complaints, legal proceedings or regulatory enquiries must not be deleted or altered outside an approved, lawful process.

13.5 Remediation and lessons learned

Material incidents must be reported to Council through an appropriately confidential process.

Council will oversee corrective actions, assign owners and review whether the incident indicates wider weaknesses in policies, systems, access controls or organisational practices.

14. Retention, disposal and information recovery

Personal information no longer required for a lawful purpose must be securely deleted, destroyed or anonymised. Archiving is permitted only where a continuing lawful purpose justifies retention.

Council will approve an information retention and disposal schedule covering membership, certification, financial, governance, complaints and operational records.

Information no longer required must be securely deleted, destroyed, de-identified or archived in accordance with that schedule.

No person may independently delete, destroy or dispose of Institute records where:

- The records remain subject to a lawful retention requirement.
- They are relevant to an active or reasonably anticipated dispute, complaint, investigation or proceeding.
- They are subject to a preservation instruction.
- Their disposal would compromise an authorised transition or record recovery process.

A documented legal or investigation hold takes precedence over ordinary disposal schedules until appropriately released.

The retention and disposal schedule recognises statutory and constitutional recordkeeping requirements.

15. Training and acknowledgement

Council officers and other individuals with access to sensitive Institute information must receive appropriate privacy and information security guidance.

Induction must cover confidentiality, authorised use, system access, incident reporting and handover obligations.

Individuals with elevated access must acknowledge their responsibilities in writing.

Training and guidance will be refreshed periodically and following material changes in policy or identified risks.

16. Compliance and breaches of policy

Compliance with this policy is mandatory for individuals acting on behalf of IMCNZ.

Suspected violations will be assessed objectively, proportionately and in accordance with applicable law, contractual terms, the IMCNZ Constitution, bylaws and relevant conduct or dispute procedures.

Possible responses may include corrective training, restriction or revocation of access, recovery of information, contractual remedies, independent investigation, disciplinary procedures or lawful referral to external authorities.

No finding of misconduct will be presumed solely from an allegation, complaint or unresolved dispute.

Individuals must not be disadvantaged for raising a genuine privacy or security concern, exercising statutory rights or cooperating with a lawful investigation.

This policy does not establish a separate disciplinary jurisdiction or authorise sanctions outside the IMCNZ Constitution, bylaws and approved complaints and dispute-resolution processes. Operational security measures may be taken where lawfully authorised and reasonably necessary to protect information assets.

17. Governance, assurance and continuous improvement

Council is accountable for ensuring that appropriate privacy and information security arrangements are implemented and maintained.

At least annually, Council will review:

- Privacy and information security risks.
- Access control arrangements and privileged accounts.
- Compliance with handover and record management requirements.
- Material incidents and corrective actions.
- Relevant service provider risks.
- Policy compliance and improvement priorities.

The Privacy Officer will report material risks, incidents and systemic concerns to Council, with appropriate safeguards for confidentiality and conflicts of interest.

Council may commission independent assurance where an incident, repeated control weakness or material governance concern warrants it.

18. Related documents and legislation

This policy should be read alongside:

- Privacy Act 2020, as amended.
- Unsolicited Electronic Messages Act 2007.
- Incorporated Societies Act 2022.
- IMCNZ Constitution and bylaws.

- IMCNZ Code of Consultant Practice.
- IMCNZ complaints and dispute resolution procedures.
- IMCNZ Records Retention and Disposal Schedule.
- IMCNZ Information Access and Handover Procedure.
- IMCNZ Privacy Breach Response Procedure.
- Applicable service provider agreements and confidentiality obligations.

This policy operates subject to applicable legislation, the IMCNZ Constitution and validly adopted bylaws. It supplements, and does not replace or amend, the constitutional provisions or duly authorised processes governing membership rights, complaints, disputes, disciplinary matters and appeals. Where an inconsistency arises, the higher governing requirement prevails.

Nothing in this provision limits IMCNZ's ability to take lawful current measures to protect records, preserve evidence or address ongoing risks.

19. Policy review

This policy will be reviewed at least annually and earlier if required following:

- Material legislative or regulatory changes.
- A significant privacy or information security incident.
- Material changes to IMCNZ systems or information processing.
- Relevant recommendations from an independent review, regulator or competent authority.

Amendments require approval by IMCNZ Council.

Approved by: IMCNZ Council
Approval date: 20 October 2026
Next review: 12 months after approval