POLICY

Dental Council
Te Kaunihera Tiaki Niho

Privacy and information

Approved: 7 April 2026
Issued: 18 May 2026
For review: 31 March 2029

Scope and purpose

1. The purpose of this policy is to set out how the Dental Council (the Council) meets its obligations under the Privacy Act 2020 and the Health Information Privacy Code 2020 when collecting, using, storing, and disclosing personal information and health information.

2. This policy applies to all personal information and health information collected by the Council, competence review committees (CRCs) and any other committees appointed by the Council to carry out regulatory functions. It does not apply to:
   - functions carried out by, or information collected by, Professional Conduct Committees (PCCs). PCCs are appointed by the Council under s 71 of the Health Practitioners Competence Assurance Act 2003 (the HPCA Act) but are a separate agency under the Privacy Act.
   - personal information collected through user activity on the Council's website (e.g. cookies or IP addresses) is covered in the *Privacy Notice* available on the Council's website: www.dcnz.org.nz.

Definitions	
Personal information	Information about an identifiable individual. Information includes the written word (whether on paper or electronically) and may include verbal discussions or records of verbal discussions.
Health information	Any personal information about an identifiable individual that relates to their health, disability, or the health services provided to them, as protected under the Health Information Privacy Code 2020.
Information Privacy Principles (IPPs):	The 13 principles in s 22 of the Privacy Act that set out how information relating to an individual can be collected, used, and disclosed.
Third party	Any person or organisation other than the individual concerned.
Regulatory functions	All functions, duties, or powers of the Council, including the functions carried out by CRCs and other appointed committees in performing their roles under the HPCA Act, unless a distinction is expressly required.

Legal context

HPCA Act

3. Section 3(1): the Council's principal purpose is to protect public health and safety by ensuring that oral health practitioners (practitioners) are competent and fit to practise.

4. Section 118(f): the Council may receive information from any person about a practitioner's practice, conduct, or competence and may act on that information.

5. Schedule 3, clause 2: the Council may receive as evidence any statement, document, information or matter, whether or not it would be admissible in a court.

Privacy legislation

6. The Council must comply with the:
   - Privacy Act 2020 (**Privacy Act**)
   - Health Information Privacy Code 2020 (**HIPC**)
   - Relevant HPCA Act requirements relating to the collection and use of personal information or health information.

Policy

7. The Council collects and manages personal information and health information in accordance with its obligations under the Privacy Act, the HIPC, and the HPCA Act, including to meet its statutory obligation to protect public health and safety and maintain professional standards. This includes obligations relating to:
   - lawful collection and use of personal information and health information
   - secure storage and proper disposal
   - rights of access and correction
   - appropriate responses to privacy breaches.

Types of information collected

8. The Council collects information necessary to perform its regulatory functions under the HPCA Act, including:
   - *Identifying information*: Names, contact details, and qualifications.
   - *Professional history*: Education, qualifications, registration, recertification and registration status
   - *Conduct and competence*: Complaints, notifications and related correspondence, and information obtained for CRC reviews
   - *Health information*: Details regarding the health of practitioners or patients, when required to assess fitness to practise, or professional standards. All health information – including health information about patients, members of the public, or practitioners – is managed in accordance with the HIPC.

9. The Council also collects information to support its administrative and management functions, and for training and quality-improvement purposes.

Methods of collection, including collection from third parties

10. The Council collects personal information and health information:
    - directly from the individual concerned
    - indirectly from third parties, including (but not limited to) complainants, notifiers, health practitioners, employers or colleagues, educational institutions, health agencies (including overseas agencies and regulators), ACC, the HDC, and the courts.

11. The Council will only collect information if it is necessary to support its regulatory functions. The Council will collect Information directly from the individual concerned or with their consent unless there is a lawful justification to collect from a third party, e.g. for competence, conduct or fitness to practise processes.

Collection from third parties and notification requirements (IPP 3A)

12. Information about the practice, conduct, fitness, or competence of a practitioner may be provided to the Council by any person or organisation. This information may be received in writing, through an online form, or verbally.

13. Where personal information is collected from a third party, the Council will notify the individual concerned as soon as practicable of:
    - the source of the information
    - the information collected
    - the purpose of collection and intended use
    - how and where the information is held; and
    - how the individual may access or correct the information

14. Notification may be delayed or withheld if permitted by IPP 3A, e.g. where notification would:
    - prejudice the purpose of collection (e.g., early-stage investigation)
    - create a safety risk
    - not be reasonably practicable.

Purpose of collection

15. Information is collected to support the Council's regulatory functions, including (but not limited to):
    - registration, practising certificates, and recertification
    - assessing complaints and notifications
    - competence reviews and disciplinary functions
    - ensuring fitness to practise
    - maintaining the public register
    - protecting public health and safety.

16. Information may also be collected for administrative purposes, including quality assurance, auditing, research, internal complaint management, and staff training.

Use and disclosure of information

17. The Council only uses or discloses information for the purpose it was collected or as authorised by law. It will not release information that would breach privacy or confidentiality obligations or that is not necessary for its regulatory functions.

18. The Council may share relevant information with:
    - CRCs, PCCs, and advisors: To carry out competence reviews or investigations, or to provide advice to the Council.
    - Relevant agencies: Such as the HDC, ACC, or overseas regulators.
    - The public:
        - certain details (name, registration status, and specific orders) must be public by law. The Council publishes this information on its public Register (available on the Council website).
        - in certain cases: the Council may publish a practitioner's name in association with any orders it makes.[1]

19. In some circumstances, Council *must* disclose information to a third party, e.g. referring a complaint alleging that the practice or conduct of a health practitioner has affected a health consumer to the HDC under s 64 HPCA Act.

20. Before information is used or shared, Council takes reasonable steps to ensure it is accurate, complete, up to date, and relevant.

Official Information Act

21. The Council is not subject to the Official Information Act 1982 (**OI Act**). However, information shared with agencies that *are* subject to the OI Act (e.g. ACC, HDC, Ministry of Health, Police) may become available through their processes.

Storage, security, and retention

22. Information is stored securely and is only accessible to staff, Council, committee members, or Council agents who need it to perform their duties.

23. The Council retains information only for as long as necessary to meet its legal, regulatory, operational and accountability obligations. Information relating to a practitioner's registration, practice, competence, conduct (including complaints or notifications), and fitness to practise is

[1] See the Council's Naming Policy for further information on this process.

relevant for as long as the practitioner is registered. It remains relevant following cancellation of registration (e.g. where the practitioner remains able to return to practise).

24. Retaining information assists the Council to (among other things):
    - protect public health and safety by ensuring it has a complete understanding of a practitioner's practice, including any possible risk of harm or risk of serious harm.
    - enable informed decisions about individual practitioners, including decisions about their ongoing practice.
    - enable informed decisions on applications for re-registration or allegations about any act or default occurring before cancellation of registration.
    - ensure the Council can respond to legal inquiries about practitioners or oral health practice.

25. If a practitioner is brought to the Council's attention on more than one occasion, all relevant information will be considered when deciding whether further action is necessary under the Council's conduct, competence or health processes.

26. When information is no longer required it is securely archived or destroyed to prevent unauthorised access.

Unique identifiers - Health Practitioner Index (HPI)

27. The HPI provides a unique identifier for each health practitioner and links practitioner information to a national database administered by the Ministry of Health. The Council supplies information to the Ministry of Health for inclusion in the HPI. This may include a registrant's full name, gender, date of birth, registration qualification, scope(s) of practice, practising status, and any conditions on practice.

28. Unique identifiers (registration numbers) are assigned only where required to support the efficient performance of the Council's regulatory functions and are not used unnecessarily.

Access and correction

29. Individuals have the right to request a copy of their information and to ask for corrections. Requests should be directed to the Council's Privacy Officer.

Withholding of Information following an access request

30. The Council may withhold information following an access request in limited circumstances permitted by the Privacy Act, including where release would:
    - pose a serious threat to health or safety
    - prejudice maintenance of the law
    - breach legal privilege

- unjustifiably disclose information about another person
- fall under any additional withholding ground in sections 49–55 of the Privacy Act.

31. Under s 50 of the Privacy Act, information that is "*evaluative material*" (e.g. confidential references) may also be withheld where releasing it would identify the source or undermine its purpose.

32. Where information is withheld, the Council will explain the reason and advise the individual of their right to make a complaint to the Office of the Privacy Commissioner.

Anonymous information

33. The Council occasionally receives information about a practitioner from individuals or agencies who wish to remain anonymous. The Council must balance this wish against the principles of natural justice, which generally require that a practitioner knows the identity of their accuser so they can respond fairly to the concerns.

34. Generally, the Council will not take formal action based solely on anonymous information. In most cases, it will simply retain the information on file for future reference. This ensures the practitioner is not unfairly penalised based on claims that cannot be verified or challenged.

35. The Council may decide to investigate or act on anonymous information if it meets one or more of the following criteria:
    - seriousness: The information contains serious allegations
    - credibility: The information is detailed, corroborated by other evidence, or relates to a matter where the source's identity isn't essential to proving the facts.
    - protected disclosures: There are clear grounds to protect the identity of the person providing the information (e.g., a "whistleblower" situation where they fear retaliation).

36. If the Council is considering acting on anonymous information, it must determine if it can do so while keeping the source anonymous. Key considerations include:
    - *Is it material?* Is the identity of the person who provided the information necessary to assess if the concern is valid?
    - *Can the practitioner respond?* Can the practitioner still provide a full and fair explanation of their alleged conduct without knowing exactly who complained?
    - *Should notification occur?* Under IPP 3A, the Council may choose *not* to tell the practitioner who the source is if doing so would create a safety risk or compromise the investigation.

37. If the Council decides to act on anonymous information, it must consider whether withholding the source of the information from the practitioner is permitted under IPP 3A, e.g. where notification would:
    - prejudice the purpose of collection (e.g., early-stage investigation)
    - create a safety risk
    - not be reasonably practicable.

38. Even if the Council chooses not to act immediately, anonymous information will be stored securely. If further concerns are raised about the same practitioner in the future, this information may be revisited to determine whether a possible pattern of behaviour is emerging that requires Council action.

Privacy breaches

39. The Council is committed to upholding high standards of privacy and information security. Despite these efforts, privacy breaches may still occur.

40. Any staff member, Council member, committee member, contractor, or other individual working with the Council who becomes aware of a privacy breach, possible privacy breach, or the potential for a privacy breach - must report it to the Privacy Officer as soon as practicable. The Privacy Officer will undertake further investigation and coordinate any required remedial action.

41. Where a privacy breach may pose a risk of serious harm to affected individuals (as assessed under s 113 of the Privacy Act), the Council will comply with the notifiable privacy breach requirements under the Privacy Act. This includes notifying affected individuals in most situations, and, where required, the Office of the Privacy Commissioner.

42. All suspected or actual privacy breaches must be promptly reported to the Privacy Officer to ensure appropriate assessment and response.

Roles and responsibilities

Role	Responsibilities
Privacy Officer	▪ Encourages and ensures compliance with the IPPs, provides advice to managers dealing with information requests made under the Privacy Act, and works with the Privacy Commissioner in connection with investigations. ▪ Provides advice and information to the Council about privacy issues or impacts when new policies or procedures are being considered, or when privacy breaches occur.
Contact information	
Privacy Officer	Corporate Services Manager
Email:	privacyofficer@dcnz.org.nz
Postal address:	PO Box 10-448, Wellington 6140, New Zealand
Telephone:	+64 4 499 4820

Making a privacy complaint

Making a privacy complaint to the Council

43. If any individual believes that their privacy has or may have been breached by the Council, they can raise their concern and/or make a complaint to the Council's Privacy Officer. A breach of privacy means a breach of any one of the 13 IPPs.

If…	Then…
An external complaint of breach of privacy is received	It should be forwarded to the Privacy Officer who will investigate the matter and reply within 20 working days of receiving the complaint, unless further time is required.
An individual does not feel the Council has handled the complaint to their satisfaction	They can make a complaint directly to the Privacy Commissioner for breach of privacy.
An individual does not wish to approach the Council	They can make a complaint directly to the Privacy Commissioner for breach of privacy.

Making a complaint to the Privacy Commissioner

44. Complaints may be made directly to the Office of the Privacy Commissioner. Information about how to make a complaint is available online at https://privacy.org.nz/your-rights/making-a-complaint/complaint-form/ or on the Privacy Commission's helpline: 0800 803 909.

Administration

Related policies

1. Notification Policy
2. Health (Fitness to practise) policy
3. Registration policy
4. Recertification policy
5. Naming policy

Version control

Policies replaced or rescinded by this policy	
CAC001	Acting on information received about OHPs policy