



Privacy & CCTV Policy

Approval Details

Policy Sponsor	Business Manager
Approval Authority	JCU Dental Board
Date for next review	December 2027

Version	Approval date	Implementation date	Details	Author
1.0	08.02.2022	08.02.2022	Privacy Policy	Company Secretary
2.0	19.04.2023	19.04.2023	Policy Update	Company Secretary JCU Legal
3.0	06.02.2024	06.02.2024	Policy Update	Company Secretary JCU Legal
4.0	09.12.2025	01.01.2026	Policy Update	Company Secretary JCU Legal
5.0	09.06.2026	09.06.2026	Policy Update	Business Manager JCU Legal

1 Policy

JCU Dental is committed to protecting the privacy of those who visit its clinic and their personal information. We will take all reasonable steps to ensure that the collection, use, disclosure and handling of all personal information complies with the *Privacy Act 1988* (Cth) [“the Act”] and the Australian Privacy Principles [“APP’s”].

JCU Dental carries out a health service and therefore must collect health information as explained within this document. We only collect health information that is necessary for one or more of our functions or activities. For the collection of health or sensitive information, we will obtain consent in addition to the collection being necessary.

A copy of this policy is available by contacting our Privacy Officer.

2 Scope

This policy applies to all clients, suppliers, patients and their families, employees, visitors, contractors, consultants and other representatives engaged by JCU Dental and to those who have a legitimate business need to access personal information in the course of performing their duties.

3 Responsibility

The obligations imposed on JCU Dental under this policy are also imposed on any individual employed or engaged by JCU Dental. If a representative of our Company discloses personal information, that individual must take steps as are reasonable in the circumstances to ensure that the third party does not breach the APPs in relation to the information.

All matters concerning information privacy (IP) are to be directed to our Privacy Officer:

Name of Person	Jeffrey Reddy
Position Title of Person	Business Manager
Telephone Number	07 4232 1412
Email Address	jeffrey.reddy@jcu.edu.au

4 Definitions

Personal Information is defined as information or an opinion about an identified individual, or an individual who is identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

Health information is any information about a person’s health or disability, and any information that relates to a health service they have received, are receiving or will receive. Health information is sensitive and personal, which is why there are laws to protect the rights of individuals in keeping their information private.

Sensitive information is a type of personal information such as: race or ethnic origin, political opinions, religious or philosophical beliefs, sexual preferences and orientation, health information and criminal record. If mishandled, this information may result in discrimination or harm.

5 Collection of Personal Information

Typical examples of personal information collected by JCU Dental include:

- Names, address, email address and telephone numbers;
- Health records including family history, diagnosis and treatment, test results, x-rays, scans;
- Medicare and other Commonwealth benefit card details;
- Financial information such as banking information;
- We may capture the IP address and device ID when accessing online services;
- Age, date of birth and gender;
- Employment related information including employment records, training, performance and conduct information, taxation, banking, superannuation details and professional associations;
- Employee, contractor and consultant personal information including addresses, contact numbers, gender, age, employment history, references, resume, medical history, criminal record, emergency contacts, qualifications and licenses;
- Resumes, contact details, references and qualifications for the purpose of assessing suitability for employment;
- Your image whilst in attendance at the clinic, through surveillance footage of the clinic for the purpose of ensuring the safety and security of our patients and employees – for further information see clause 11 below; and
- General correspondence and/or notes detailing conversations.

Personal information will be collected directly from the individual whose information it is. However, there may be circumstances (e.g. due to health) where we may need to collect information from, or talk to someone else, for example the individual's medical representatives, attorney, carer or a relative.

In delivering health services, we will only collect health information with the patient's consent to do so. Consent may be express or implied. However, consent may not be required if:

- The collection is required or authorised by an Australian law or court order;
- Collection of information is necessary to prevent a serious threat to the life, safety or health; or
- The information is necessary to provide a health service to the individual, and the collection is performed in accordance with the rules of a competent health or medical body (for example, the Medical Board of Australia or the Royal Australian College of General Practitioners).

6 Data Protection

JCU Dental uses a variety of security measures to help prevent unauthorised access to, an improper use of personally identifiable information.

Our employees and other representatives are required to take steps as are reasonable in the circumstances to protect the personal information from misuse, interference, loss and from unauthorised access, modification or disclosure. Our security measures include:

- Training our employees in privacy matters;
- Limiting or restricting access to information to those with a legitimate need;

- Physical security of documents in locked rooms and filing cabinets;
- Appropriate building security and access controls;
- Tracking of any information being shipped or posted;
- Password protection on all electronic and wireless devices;
- Regular and continuous monitoring of our IT systems;
- Installation and maintenance of firewalls to prevent hacker attacks;
- Installation and maintenance of anti-malware programs on computers and servers;
- Restricting the ability of users to download unauthorised software onto our systems;
- Limited remote access to our systems by approved users;
- Restriction and secure storage of laptops/notepads to those employees who need them;
- Secure access to digital documents held on our printers; and
- Obtaining consent for the use of photographs that identify any individual.

If we hold personal information that we are not required by law to retain the information, we will take such steps as are reasonable in the circumstances to destroy the information or to ensure it is de-identified within the timeframes stipulated by any relevant authorities or retention schedules.

Where JCU Dental has reasonable grounds to believe that an eligible data breach (as defined in legislation) has occurred, or in instances where it is directed to do so by the Commissioner, it will provide relevant notification to the Office of the Australian Information Commissioner (OAIC) and/or to affected individuals.

7 Use of Personal Information

We use the personal information we collect in connection with our activities and functions, such as:

- Providing dental services and diagnosis;
- Responding to requests and communicating with individuals;
- Processing payments for dental services;
- Providing tailored content in publications, email, social media and on the web;
- Performing data analytics to improve our service offerings;
- Payroll, workers compensation, superannuation contributions, and any assessments of fitness for duty for employment purposes;
- Ensuring the safety of our patients and employees;
- Complying with and enforcing applicable legal, industry or government requirements, contractual obligations and our policies and procedures; and
- For any other purpose that we may specifically disclose at the time the information is collected.

We will comply with the requirements in relation to the *Spam Act 2003* (Cth) in relation to our commercial communications.

8 Disclosure of Personal Information

There may be occasions where we may need to share personal information with third parties in order to carry out our activities and functions in circumstances such as:

- Third parties providing recruitment, training, human resources, payroll or other services to us;
- — Legal, industry or government requirements to share information about particular health conditions

or statistical information;

- Provision of information to police or subpoenaed information for a court case;
- Law enforcement agencies where the personal information is reasonably necessary for a law enforcement activity;
- Certain government agencies (e.g. Australian Tax Office, Centrelink, WorkCover); and
- To our legal, insurance, financial and business advisors.

We will ensure that any such disclosure is limited to only what is necessary.

All third parties are required to maintain the confidentiality of personal information provided to them by us and are only authorised to use the information for the purpose for which it was collected.

9 Currency of Personal Information

We have an obligation to maintain the currency of personal information held by us, and in connection with the provision of ongoing services or business requirements.

We maintain procedures which may require individuals to update their personal information with us from time to time, and as advised by us.

10 Access to Personal Information

An individual may request to access their own personal information provided to us. In such instance, we will ask for the following:

- Request is to be made in writing to the Privacy Officer.
- Personal identity is verified as we require.
- Rightful access to the information is established.

External persons (e.g. a relative) may only access an individual's personal information in instances where the individual is incapacitated, and where they have a legitimate right to access such information. In such instances, we may require evidence of their entitlement to request such information (e.g. provision of the enduring power of attorney).

In accordance with the provisions of APP #12, there are certain circumstances in which JCU Dental may refuse to grant an individual access to personal information. In such situations, we will provide the individual with written notice that sets out:

- the reasons for the refusal; and
- the mechanisms available to the individual to make a complaint.

You may update your personal information by emailing jeffrey.reddy@jcu.edu.au.

11 CCTV Surveillance

JCU Dental is also committed to providing a safe and secure environment for our patients, staff, students and visitors. To support this commitment, Closed Circuit Television ("CCTV") cameras are installed in designated areas of our clinic.

For the avoidance of any doubt, James Cook University (JCU) owns and operates the CCTV cameras on JCU and JCU-managed premises and JCU Dental is a JCU-managed premises.

Purpose of CCTV

CCTV is used to:

- Enhance the health, safety and security of patients, staff, students, and visitors.
- Deter and manage antisocial, unlawful, or aggressive behaviour.
- Support the investigation of incidents or accidents on site.
- Assist in the protection of property and infrastructure.
- CCTV is **not** used for monitoring the clinical care of patients, private consultations, teaching or assessment purposes and does not replace effective personal communication.

Privacy and Confidentiality

We understand the importance of protecting the privacy and dignity of individuals. All CCTV use complies with the following:

- *Privacy Act 1988* (Cth).
- Australian Privacy Principles (APPs).
- State-based surveillance legislation.

Cameras are not installed in private areas such as:

- Bathrooms.
- Changerooms.

Cameras may be in place at:

- Main entrances and exits.
- Waiting rooms.
- Reception areas.
- Clinical areas.
- Corridors.

Clear CCTV camera signage is displayed in the clinic's reception area.

Recording and Storage

- CCTV footage is recorded and stored securely using encrypted systems.
- Access is restricted to authorised personnel only (e.g. Privacy Officer/Business Manager, Company Secretary, senior clinic management, JCU Security).
- Recordings are stored for a limited time (approximately 30 days), unless required for a specific investigation or legal reason.
- Footage may be provided to law enforcement or insurers where legally appropriate.

Access to Footage

CCTV footage will only be accessed where reasonably necessary for:

- Work, health and safety incidents;
- Security incidents or complaints; and/or
- Investigations authorised by the clinic and/or JCU.

CCTV footage may be disclosed only where required or authorised by law, including to:

- Queensland Police Service or other law-enforcement agencies;
- Courts or tribunals; and/or
- Regulators or insurers (where applicable).

Footage will not be used for any unrelated or secondary purpose.

Individuals may request access to footage in which they appear by submitting a written request to the our Privacy Officer. Access will be considered in line with relevant legislative requirements and may be refused where it compromises the privacy of others or relates to an ongoing investigation.

Review and Compliance

This policy is reviewed annually or whenever significant technological, legislation, or risk assessment changes occur. CCTV use is part of our broader security and workplace safety strategy and aligns with relevant JCU policies and procedures and guidance from the Australian Health Practitioner Regulation Agency, Australian Dental Association and Dental Board of Australia.

For questions about CCTV utilised in our clinic, please contact our Privacy Officer.

12 Complaints

Individuals have a right to complain about our handling of personal information or use of CCTV technology if the individual believes that JCU Dental has breached the Act or APPs.

If an employee or representative of JCU Dental becomes aware of an individual wanting to make a complaint to us about a privacy matter, the employee or representative should direct the individual to contact our Privacy Officer. The Privacy Officer will investigate the complaint and will provide a response to the complainant within a reasonable period of time.

Individuals who are dissatisfied with our response to a complaint, may refer the complaint to the Office of the Australian Information Commissioner.

13 Breach of this Policy

An employee, contractor or other representative employed or engaged by us to carry out an act or activity which involves the handling of personal information, is responsible for ensuring that in doing so, they comply with the obligations imposed on JCU Dental.

Any breach to this policy may result in disciplinary action up to and including termination of employment or discontinuance of other contractor/supplier agreement.

14 Associated Documents

- *Privacy Act 1988* (Cth)
- Australian Privacy Principles
- *Information Privacy Act 2009* (Qld)
- *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)
- *Spam Act 2003* (Cth)
- *My Health Records Act 2012* (Cth) – for the health sector
- *Healthcare Identifiers Act 2010* (Cth) – for the health sector
- *James Cook University Security Policy (CCTV)*