Australia and New Zealand Privacy Policy and Procedure

1 Introduction

Dentsply Sirona Pty Ltd, hereafter referred to as 'the company' will endeavour to use all reasonable efforts to protect the privacy of an individual's Personal Information and to comply with any obligations imposed on the company by the Australian *Privacy Act 1988* (Cth) and the New Zealand *Privacy Act 1993* (as that Act may be amended or superseded from time to time) (**Privacy Acts**), the thirteen Australian Privacy Principles (**APP**) twelve New Zealand Information Privacy Principles (**IPP**).

The Company will take reasonable steps to:

(a) collect, hold, store, manage, use and disclose Personal Information in a lawful, fair and transparent manner;

(b) protect the confidentiality and privacy of Personal Information collected or held by the company through the implementation of appropriate storage and security measures;

(c) enable individuals to access and seek correction of their Personal Information; and

(d) provide an internal mechanism for complaints about breaches of the APP or IPP or this policy.

The company will make this policy available via its web site to all job seekers, employees, volunteers, contractors, subcontractors, consultants, clients, customers and any other person to whom it may be relevant.

A Privacy Statement is also available on the website.

2 Purpose

The purpose of this policy is to:

(a) meet the company's obligations under the Privacy Acts, the APP and the IPP;

(b) inform interested persons about the company's practices in relation to the handling of Personal Information; and

(c) provide a mechanism for complaints about breaches of the Privacy Acts, the APP, the IPP or this policy.

3 Scope

This policy applies to the collection, holding, storage, management, use and disclosure of all Personal Information by the company.

This policy may be relevant to you if you are:

(a) a client or customer of the company;

(b) seeking employment with the company;

(c) an employee of the company;

(d) a contractor, subcontractor or consultant to the company;

(e) a supplier or vendor of goods or services to the company; or

(f) any other individual whose Personal Information may be given to, or held by, the company.

This policy does not address specific employment issues that may relate to privacy. These matters may be covered in other company policies.

4 Anonymity and pseudonymity

4.1 The APP gives individuals the option of not identifying themselves, or using a pseudonym when dealing with the company, unless:

(a) the company is required or authorised by law to deal only with individuals who have identified themselves; or

(b) it is impracticable to deal with individuals on an anonymous basis or who are using a pseudonym.

4.2 Where possible the company will endeavour to provide ways for individuals to deal with the company anonymously or using a pseudonym. However, in many circumstances this may not be possible, and we may need to establish your identity in order to give you advice, goods or services and/or undertake our company's functions and activities.

5 Collection of personal information

5.1 **Why does the company collect Personal Information?**

We collect Personal Information from individuals for a range of reasons related to our functions and activities, including but not limited to:

(a) general administrative purposes;

(b) proof of identity purposes;

(c) account administration, including ordering and courtesy calls and the administration of payments and services;

(d) billing purposes;

(e) research and analysis;

(f) direct marketing;

(g) providing services in culturally appropriate ways and with an awareness of individual differences;

(h) statistical purposes;

(i) to assist in monitoring, reviewing and improving customer service;

(j) establishing and maintaining client and customer records;

(k) regulatory compliance purposes;

(l) workplace health and safety purposes;

(m) employment and recruitment related purposes, including managing candidates for opportunities;

(n) determining eligibility for various services; and

(o) to assist in the provision of information, advice and/or goods and services to customers and clients.

5.2 **What kinds of Personal Information does the company collect?**

The company needs to collect certain Personal Information about various individuals in order to properly carry out its functions and activities. The types of information that the

company collects will depend on the circumstances of the individual's involvement or contact with the company.

Some examples of the types of information that the company routinely collects, and the basis for collection includes:

(a) for the purpose of opening a credit account to order products and services from us, the management of that account and of our relationship with you, including ensuring delivery of ordered products via freight providers, we collect the following types of information:

    (i) name, address, phone, fax, email address, business trading name and ABN, length of time at business address, shipping information (including any alternative shipping address) Provider Number, Registration number and State in which registered, year of graduation, credit card details, type of practice / specialty, number of practitioners, number of hygienists, trade references (name, phone and fax details), Company information including name, ACN, registered office, date and state of incorporation, authorised capital and paid up capital, poisons licence number and directors full names and addresses, application witness name and address details, personal guarantee;

(b) for the purpose of account management (including management of payments) and managing our business relationship with you, including personalising communication and providing relevant information, organising maintenance or technical service calls, allocating Specialists to your account and technicians to your service requirements, responding to questions and comments and providing advice and support relating to goods and services to customers, we may collect the following types of information:

    (i) name, job title, customer account number, address, phone, fax, email, business trading name, registration number, credit card details, products ordered, personal opinions, experience with Dentsply Sirona products or services and disclosed personal information e.g. birthdays, special events;

(c) for the purpose of managing product returns and complaint resolution, including regulatory reporting requirements, we typically collect the following types of information. This information may also be used for the purposes of research and product development to help us improve our products:

    (i) name, customer number, invoice number, personal opinion, de-identified patient information (age and sex) and experience with Dentsply Sirona products or services;

(d) for the purpose of entering into a business agreement, we may collect the following types of information:

    (i) name (of individual), job title, department, name of organisation, address, phone, fax, email, business trading name and ABN, insurance status

(e) for the purpose of ensuring that clients receive relevant promotional material, we may collect the following types of information:

    (i) Customer number, customer address details, name, business name, occupation, address, phone, fax and email, and experience with Dentsply Sirona products or services.

(f) For the purpose of ensuring client access to the Company estore (for online purchasing), we may collect the following types of information:

(i) Customer contact details i.e. customer & business name, address, email address, customer registration number, experience with Dentsply Sirona products or services and phone number. This information is collected for all customer groups, including students.

(g) For the purpose of ensuring that estore customers who do not have an account with Dentsply Sirona have access to the estore, the following additional information is also collected:

(i) Credit card type, name on credit card, credit card number, expiry date and CVV/CVC number.

(h) For the purpose of processing credit card payments for orders placed by phone, the following additional information is collected:

(i) Credit card number and expiry date.

(i) For the purpose of administering, updating and maintaining our website and our estore, including optimising customer experience in using the estore, helping diagnose problems with our server and compiling broad statistical data, the following additional information is also collected:

(i) Username and password, history of interactions with you, your purchases from us and information about the use of our products, and other information such as demographic data and shopping behaviour and preferences.

(j) For the purpose of facilitating and advertising the assistance of Key Opinion Leaders (KOLs) with offering training to clients, we may collect the following types of information (including within KOL agreements):

(i) Photographs and comments, title, name, company name and address details, agreed type of work to be undertaken & $ payment value per nominated duration, agreement inclusions & exclusions (T&Cs).

(k) For the purpose of providing and advertising Clinical Education programs i.e. clinical training programs for clinicians, we may collect the following types of information:

(i) Photographs and comments, title, name, company name, address, customer number, phone (office or mobile), address, email address amount to be paid and credit card details (including credit card type, name on credit card, credit card number, expiry date and CVV/CVC number.

(l) For the purpose of manufacture of products for you and/or for distribution of products to you:

(i) Information about the physical condition or health of an individual may be provided by the individual or by a healthcare professional.

(m) Information outlined above may also be used as appropriate for compliance, legal, regulatory and ethical purposes:

(i) For example, to enforce our Terms and Conditions or other legal rights, comply with applicable laws, regulations and request from governmental agencies and comply with industry standards and our policies.

5.3 **Who does the company collect Personal Information in relation to?**

The company collects Personal Information in relation to a range of individuals, including but not limited to:

(a) clients or customers of the company, and personnel employed by those clients or customers;

(b) persons seeking employment with the company;

(c) referees to clients, customers and persons seeking employment with the company;

(d) employees of the company;

(e) contractors, subcontractors and consultants to the company;

(f) suppliers or vendors of goods or services to the company; and

(g) any other persons who have dealings with the company.

5.4 **How does the company collect Personal Information?**

The company will only collect Personal Information by lawful and fair means.

Personal Information is collected through a variety of channels, including but not limited to:

(a) paper forms or notices;

(b) online portals and mechanisms, including our website and estore;

(c) face to face;

(d) over the phone; and

(e) electronic or paper correspondence.

5.5 **Who does the company collect Personal Information from?**

Typically, the company will only collect Personal Information about an individual from that individual.

However, it may be necessary from time to time to collect Personal Information about an individual from someone other than the person themselves. This might happen where:

(a) the individual has consented to the collection of the information from someone else;

(b) the company is required or authorised by law to collect the information from someone else; or

(c) it is unreasonable or impracticable to collect the information from the individual personally.

Examples of third parties that we may collect Personal Information from include, but are not limited to, our business partners or related entities, family members, medical advisers, current and former employers, educational institutions, banks and financial institutions, the Australian Securities and Investments Commission, Medicare, Centrelink, the Department of Fair Trading, the Australian Tax Office, Work Cover, government departments, government agencies and private organisations.

5.6 **When will the company collect Personal Information?**

The company will only collect Personal Information (excluding Sensitive Information) about an individual if the information is reasonably necessary for, or directly related to, one or more of the company's functions or activities.

The company will only collect Sensitive Information about an individual if:

(a) the individual consents to the collection of the information and the information is reasonably necessary for one or more of the company's functions or activities;

(b) the collection of the information is required or authorised by or under an Australian or New Zealand law or a court/tribunal order; o

(c) a Permitted General Situation or a Permitted Health Situation exists in Australia in relation to the collection of the information.

5.7 **Dealing with Unsolicited Information**

If the Company receives Unsolicited Information about an individual that the company could not have obtained by lawful means (and the information is not contained within a Commonwealth record), the company will destroy or de-identify the information as soon as practicable and in accordance with the law, noting that resumes received unsolicited will be treated as an application and handled in accordance with Section 8.1 (Individuals Seeking Employment).

Where the company could have lawfully obtained the Unsolicited Information, the company will be entitled to hold, use and disclose that information in accordance with the provisions of this policy and the APP.

5.8 **Notification of collection of Personal Information**

Where the company intends to collect, or has collected, Personal Information regarding an individual, the company will take all reasonable steps to notify or make the individual aware of:

(a) the company's identity and contact details;

(b) the purpose for which the information is or was collected;

(c) the main consequences (if any) for the individual if all or some of the information is not collected by the company;

(d) the identity of other entities or persons to whom the company usually discloses information, of the kind collected, to;

(e) this policy (in particular the sections regarding how to access and seek correction of information held by the company and how to make a complaint about an alleged breach of the APP or IPP);

(f) whether the company is likely to disclose the information to overseas recipients and if practicable to specify the countries in which such recipients are likely to be located, in the notification or by otherwise making the individual aware of those countries;

(g) where the information has been collected from someone other than the individual, or the individual may not be aware that the company has collected the information – the fact that the company has collected the information and the circumstances of that collection; and

(h) where the collection of the information is required or authorised under an Australian or New Zealand law or a court/tribunal order – the fact that the collection is so required or authorised, and the name of the law or details of the order that requires or authorises the collection.

The company will take the above steps at, or before, the time of collection or otherwise as soon as reasonably practicable after the collection of the Personal Information.

6 Use and disclosure of Personal Information

6.1 For what purpose will the company use or disclose Personal Information?

The way in which the company uses or discloses an individual's Personal Information will vary depending on the purpose for which it was collected.

For example, personal Information is routinely used or disclosed for the following purposes:

(a) proof of identity purposes;

(b) complaints management;

(c) managing and responding to requests for information;

(d) recruitment and employment related purposes;

(e) facilitate the provision of goods or services (including transport via freight providers), or to provide expanded services;

(f) direct marketing; and

(g) debt collection.

Subject to the remaining provisions of this section 7 and section 9 (Direct marketing), Personal Information will not be used or disclosed for a purpose unrelated to the purpose for which it was originally collected.

6.2 Use or disclosure for secondary purposes

Where the company holds Personal information about an individual that was collected for a particular purpose (the primary purpose), the company will not use or disclose that information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use of their Personal Information for the secondary purpose;

(b) the individual would reasonably expect the company to use or disclose the information for the secondary purpose and the secondary purpose is related to the primary purpose (or in the case of Sensitive Information, directly related to the primary purpose) (for example, we may use or disclose personal information to protect the security or integrity of our business, including our databases and systems, or for the purposes of a joint venture, collaboration, financing, sale, merger, reorganisation, change of legal form, dissolution or similar event);

(c) the use or disclosure of the information is required or authorised by or under an Australian or New Zealand law or a court/tribunal order;

(d) a Permitted General Situation or a Permitted Health Situation exists in relation to the use or disclosure of the information in Australia;

(e) the company reasonably believes that the use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(f) the use or disclosure is otherwise required or authorised by law.

Where the company uses or discloses information in accordance with section 7.2(e), it will make a written note of the use or disclosure.

The above provisions do not apply to use or disclosure of Personal Information for the purpose of direct marketing (see section 9 below instead).

7 Collection, use and disclosure of Personal Information for employment purposes

The company places great emphasis on protecting the privacy of Personal Information collected in respect of prospective, current and former employees. The provisions of this clause are intended to provide additional information in relation to the company's handling of Personal Information relating to prospective, current and former employees and to supplement the other provisions of this policy.

7.1 Individuals seeking employment

Typically, we collect the following types of information from or in relation to individuals (please note that this list is not exhaustive and additional information may be collected from time to time):

(a) name, address and contact details;

(b) proof of citizenship or work entitlement;

(c) resumes;

(d) qualification and education details;

(e) criminal record;

(f) medical history;

(g) work history;

(h) oral and/or written references; and

(i) Information disclosed as part of an employment application e.g. gender, ethnicity.

Information may be collected from the individual themselves or from other third parties in accordance with section 6.5 above.

The information we collect is primarily used to evaluate individual interest in employment and to make contact regarding possible employment with Dentsply Sirona, determine eligibility and suitability for employment by the company or any of its related entities (including but not limited to conducting qualification, reference and criminal history checks), process an application, monitor recruitment statistics and comply with government reporting requirements.

Dentsply Sirona will retain applications of unsuccessful candidates for a reasonable period after the application process to enable us to contact the candidate if another suitable position arises or to comply with our legal obligations.

7.2 Current and former employees

The company is legally required to keep various records about matters relating to the employment of both current and former employees. Such records necessarily include Personal Information.

It is important for employees to understand that the Australian Privacy Act and the APP do not apply to Employee Records.

As such, many of the provisions of this policy do not strictly apply to Personal Information held, stored, used or disclosed or otherwise handled by the company for employment related purposes and information or activity which falls within the definition of Employee Records.

Despite this, the company may at its discretion elect to comply with the terms of this policy in relation to Employee Records. If the company makes that election, which it can make and revoke at any time, it will permit employees to:

(a) request access to Personal Information held about the employee in accordance with section 12;

(b) request corrections to Personal Information held about the employee in accordance with section 13; and

(c) make a complaint about the collection, holding, storage, use or disclosure of their Personal Information in accordance with section 14.

Nothing in this section 8.2 is intended to confer any contractual or other entitlement on an employee, and an employee's rights in relation to the collection, holding, management, storage, use and disclosure of their Personal Information are strictly limited to any rights contained within the Australian Privacy Act or other applicable legislation.

8 Direct Marketing

The company will only use or disclose Personal Information about an individual for the purposes of direct marketing in accordance with this section 9 (or otherwise as may be permitted by law).

8.1 Use of Personal Information for direct marketing

The company is permitted to use or disclose Personal Information (excluding Sensitive Information) about an individual for the purposes of direct marketing, if either the information was collected:

(a) directly from the individual with their consent in circumstances where the individual would reasonably expect the company to use or disclose the information for the purpose of direct marketing and the:

  (i) company has provided the individual with a simple means to easily 'opt-out' of direct marketing communications; and

  (ii) individual has not opted out; or

(b) from someone other than the individual (or in circumstances where the individual would not reasonably expect the company to use the information for direct marketing purposes), and:

  (i) the individual has consented to the use or disclosure of the information for direct marketing purposes (or it is impracticable to obtain that consent);

  (ii) the company has provided the individual with a simple means to easily 'opt-out' of direct marketing communications;

  (iii) in each direct marketing communication, the company includes a statement that the individual may opt out of the direct marketing communications or otherwise draws the individual's attention to the fact that they can make such a request; and

  (iv) the individual has not made a request to opt-out.

8.2 Use of Sensitive Information for direct marketing

The company will only use or disclose Sensitive Information about an individual for the purposes of direct marketing if the individual has consented to the information being used or disclosed for the purpose of direct marketing.

8.3 An individual's rights in relation to direct marketing

There are certain instances when the company may use an individual's Personal Information for the purpose of direct marketing. Specific instances include but are not limited to:

(i) eBlast communication. In this instance, the company may send out emails for the purpose of updating customers on upcoming CE programs, new products or similar information.

(ii) Administration of direct mail. In this instance, the company may provide a mail house with the following data for the purpose of a direct mail campaign:

- Customer and business name, address, phone numbers and email address.

If the company uses an individual's Personal Information for the purpose of direct marketing, the individual may request that the company:

(a) not provide direct marketing communications to the individual in future;

(b) not disclose or use the information for direct marketing purposes in the future; and/or

(c) provide the individual with the source of the information.

The company will not impose any charges on an individual for making a request under this section and will endeavour to give effect to the request within a reasonable period of time.

This section 9.3 does not limit the company's obligations under other laws.

9 Cross border disclosure of Personal Information

9.1 Likelihood of disclosure

The company may from time to time disclose Personal information to overseas recipients, for example, the company's foreign related entities throughout the Dentsply Sirona group, offshore IT providers (in Indonesia[1]), and/or its foreign legal or other advisers.

The limited personal information collected for the purpose of product complaint resolution may be disclosed to relevant foreign related manufacturing entities. Foreign manufacturing entities are currently located in the following locations: USA, UK, Switzerland, France, Sweden, Italy, Germany, Brazil, Pakistan, Mexico and China.

9.2 Requirements in the event of disclosure

Subject to the exceptions set out below, if the company does disclose Personal Information to an overseas recipient, before disclosing the information, the company will take all reasonable steps to ensure that the overseas recipient does not breach the APP or IPP.

The above requirement will not apply where:

(a) the company reasonably believes that the overseas recipient is subject to laws similar to the APP and IPP and there are mechanisms that the individual can access to take action to enforce the protections afforded by such laws;

[1] Please note, Personal information is primarily managed within Australia. Access to off-shore IT providers would only be granted for limited periods for the purpose of website development and/or testing.

(b) the individual consents to the disclosure of the information to the overseas recipient after being expressly informed by the company that if the individual consents the company will not be required to take reasonable steps to ensure that the overseas recipient does not breach the Privacy Acts, the APP's and the IPP's in relation to the information;

(c) the company reasonably believes the disclosure is required or authorised by or under an Australian or New Zealand law or a court/tribunal order;

(d) a Permitted General Situation exists in Australia (other than the situations set out in section 4.7(d) or (e) above); or

(e) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

10 Integrity of Personal Information

10.1 Quality of Personal Information

The company aims to ensure that the Personal Information it collects, holds, uses and discloses is accurate, complete and up-to-date.

Individuals have the right to access and request correction of their personal information held by the company. An individual should contact the company (via the details set out in section 12.2 below) if they believe that the Personal Information that the company holds about them is not accurate, complete or up-to-date.

10.2 Security of Personal information

The company is committed to keeping Personal Information secure. To this end, the company will take all reasonable steps to ensure that Personal Information held by the company is protected from misuse, interference, loss, unauthorised access, modification or disclosure, including appropriate physical, technical and organisational security measures designed to safeguard and secure any information you provide to us.

The company's security measures include, but are not limited to:

(a) training employees on their obligations with respect to Personal Information;

(b) the use of encrypted files, firewalls, virus scanning tools and passwords to protect against unauthorised interference and access to electronically stored Personal Information;

(c) backup of electronic systems to protect against data loss;

(d) the implementation of policies and procedures regarding the appropriate use of the company's information and communication technology systems, databases and equipment;

(e) security systems in relation to paper records;

(f) secure access to the company's premises;

(g) regular audits of security systems; and

(h) requiring consultants, contractors and subcontractors to comply with the APP, IPP and this policy.

10.3 Destruction of Personal Information

The company will retain information collected for the purpose of opening and operating a credit account (including information required for account management and payments of accounts) for the duration of our business relationship until the customer requests that

the account is closed and for a period of time thereafter as required by applicable local law or where we have a legitimate and lawful purpose.

The company will, where systems allow, endeavour to destroy or de-identify Personal Information that is no longer needed by the company, as soon as practicable after the company ceases to need such information (provided the company is not required to retain it under an Australian or New Zealand law or a court/tribunal order).

11 Access to, and correction of, Personal Information

11.1 Right to request access to information

Where the company holds Personal Information regarding an individual, an individual is entitled to request access to that information.

Responding to this type of request can be a time consuming exercise. The company may be able to get the information that you require more quickly if you area as specific as possible in your request e.g. “I would like a copy of my personal data contained in my customer account file” or if you would like a copy of a particular document it would be helpful if the document is described carefully including the title, creation date, author and likely place of storage. This will help us respond to your request as quickly as possible. You may be asked for further details to assist us if insufficient information is provided.

11.2 Process for requesting access

Requests for access to Personal Information must be made in writing by contacting:

Privacy Officer c/o Regulatory Affairs

Dentsply Sirona Pty Ltd

11-21 Gilby Road

Mount Waverley

VIC 3149

ANZPrivacyOffice@dentsplysirona.com

11.3 Dealing with requests

Where a request is made, the company will endeavour to respond to the individual’s request and give access to the requested information within a reasonable time frame (but generally within 15 business days). If the request will take longer than 15 business days, contact will be made with the individual to provide the anticipated time frame for responding to the request, and the explanation for the additional time required.

Individuals will be required to provide proof of identify before information is released.

11.4 Access charges

The company may impose a charge on an individual for giving access to Personal Information. Such charges will not be excessive or unreasonable.

11.5 Refusing requests

The company will not be required to grant an individual’s request to access Personal Information where:

(a) the individual is not able to provide reasonable evidence of their identity;

(b) the company reasonably believes that giving access to the information would pose a serious threat to the life, health or safety of any individual (or a public health or public safety);

(c) giving access would have an unreasonable impact on the privacy of other individuals;

(d) the request for access is frivolous or vexatious;

(e) the information relates to existing or anticipated legal proceedings between the company and the individual, and would not be accessible by the process of discovery in those proceedings;

(f) giving access would reveal the intentions of the company in relation to negotiations with the individual in such a way as to prejudice those negotiations;

(g) giving access would be unlawful;

(h) the company is required or permitted to deny access under an Australian or New Zealand law or a court/tribunal order;

(i) the company has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the company's functions or activities has been, is being or may be engaged in, and giving access would be likely to prejudice the taking of appropriate action in relation to that matter;

(j) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(k) giving access would reveal evaluative information generated within the company in connection with a commercially sensitive decision making process.

Where a request is refused, the company will:

(a) provide the individual with a written notice setting out the reasons for the refusal and the mechanisms available to the individual to complain about the refusal; and

(b) give consideration to ways in which the request could be granted that would still meet the needs of the individual and the company (for example, by disclosure to an agreed intermediary),

unless it is unreasonable to do so in the circumstances.

12 Correction of Personal Information

12.1 Requesting a correction

If you are of the view that the Company holds personal information about you that is inaccurate, incomplete, out-of-date, irrelevant or misleading, you should notify the company in writing and ask for the information to be corrected.

12.2 Correcting information

If the company is satisfied that the information is inaccurate, incomplete, out-of-date, irrelevant or misleading, the company will take reasonable steps to correct the information.

The company may correct information even where there has been no request by the individual concerned.

12.3 Notification of correction to third parties

If the company corrects Personal Information about an individual that the company has previously disclosed to another entity or person, and the individual requests the company to notify the other entity or person of the correction, the company will take all reasonable steps to comply with such a request (unless it is impracticable or unlawful to do so).

12.4 **Refusing to correct information**

If the company refuses to correct Personal Information following a request by an individual, the company will give the individual a written notice that sets out:

(a) the reasons for the refusal;

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.5 **Request to associate a statement**

If:

(a) the company refuses to correct Personal Information as requested by the individual; and

(b) the individual requests the company to associate with the information a statement of the correction sought but not made i.e. that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading,

the company will take all reasonable steps to associate such a statement in a way that will make the statement apparent to users of the information.

13 Complaints handling

13.1 **How to make a complaint**

If you believe that the company has breached the APP, IPP or this policy in our collection, holding, management, storage, use or disclosure of your Personal Information you are able to make a complaint about the matter.

Complaints can be made in writing to:

Privacy Officer c/o Regulatory Affairs

Dentsply Sirona Pty Ltd

11-21 Gilby Road

Mount Waverley

VIC 3149

ANZPrivacyOffice@dentsplysirona.com

13.2 **How the company will deal with your complaint**

In the event of a complaint made to the company, we will contact the complainant as soon as reasonably practicable to obtain further information in relation to the complaint and discuss the process that the company intends to adopt to investigate and resolve the particular complaint.

The company will endeavour to investigate and resolve all complaints within a reasonable timeframe (generally within 14 days) and will provide the complainant with a written response to their complaint following the completion of the investigation. If the response to a complaint will take longer than 14 days, contact will be made with the individual to provide the anticipated time frame for responding and an explanation for the time frame required.

The response will include the outcome of the investigation, any proposed action that the company intends to take as a result of the outcome and details of how to dispute the outcome of the investigation.

The company may use the information obtained through the complaint process to provide feedback to staff and improve the delivery of our services.

13.3 **External complaint mechanism**

If you are not happy with the way in which the company has handled your complaint, or the outcome of the complaint, you can make a complaint to the Office of the Australian Information Commissioner or the New Zealand Privacy Commissioner as applicable.

Complaints can also be made to the Commissioner without needing to first make a complaint directly to the company.

Complaints can be made to the Australian Commissioner in the following ways:

Online: http://www.oaic.gov.au/privacy/making-a-privacy-complaint

By email: enquiries@oaic.gov.au

By phone: 1300 363 992

By fax: +61 2 9284 9666

By post: Office of the Australian Information Commissioner

GPO Box 5218, Sydney NSW 2001

or

GPO Box 2999, Canberra ACT 2601

Complaints can be made to the New Zealand Commissioner in the following ways:

- Online: https://www.privacy.org.nz/your-rights/making-a-complaint/complaint-form/
- By email: enquiries@privacy.org.nz
- By phone: 0800 803 909
- By post: Office of the Privacy Commissioner

  PO Box 10094,

  Wellington 6143

14 Breach of policy by workers

Employees, volunteers, consultants, contractors and subcontractors (collectively, "**workers**") must ensure that they:

(a) comply with the requirements of this policy during the course of their employment/engagement with the company; and

(b) do not engage in any conduct which could put the company in breach of this policy, the APP or the IPP.

In the event that a worker engages in conduct which (in the reasonable opinion of the company) puts the company in breach of this policy, the APP or the IPP, they may be subject to disciplinary action (which could include termination of employment or termination of their service contract, as the case may be).

15 Notifiable Data Breach Scheme

If there is a loss, or unauthorised access or disclosure of your personal information that is likely to result in serious harm to you, the company will investigate and notify you and

the Australian Information Commissioner as soon as practicable, in accordance with the Australian Privacy Act.

16 Updates to our privacy statement

We may at any time in our sole discretion revise or update this Privacy Policy and procedure or our privacy statement. We will indicate at the top of the documents when they were most recently updated. All changes are effective immediately when they are posted. It is your responsibility to check this Privacy Policy periodically for changes. Your continued engagement with the company following notification of any changes to this Privacy Policy constitutes acceptance of those changes.

17 Definitions

17.1 What is "Personal Information"?

Personal Information is information or an opinion about an identifiable individual, or an individual who is reasonably identifiable, irrespective of whether the information or opinion is:

(a) true or not; or

(b) recorded in a material form or not.

A reference to Personal Information includes both Sensitive Information and Health Information unless otherwise indicated.

17.2 What is "Health Information"?

Health Information is:

(a) Personal Information about:

(i) the health, including an illness, disability or injury (at any time) of an individual;

(ii) an individual's expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual;

(b) other Personal Information collected to provide, or in providing, a health service;

(c) other Personal Information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances; or

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

17.3 What is "Sensitive Information"?

Sensitive Information is:

(a) Personal Information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record;

(b) Health Information about an individual;

(c) genetic information about an individual that is not otherwise Health Information;

(d) biometrical information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

17.4 **What is "Unsolicited Information"?**

Unsolicited Information is all Personal Information received by the company that the company did not actively seek to collect.

17.5 **What is an "Employee Record"?**

An Employee Record is a record of Personal Information relating to the employment of an employee.

Examples of Personal Information relating to the employment of the employee are Health Information about the employee and Personal Information including but not limited to all or any of the following:

(a) the engagement, training, disciplining or resignation of the employee;

(b) the termination of the employment of the employee;

(c) the terms and conditions of employment of the employee;

(d) the employee's personal and emergency contact details;

(e) the employee's performance or conduct;

(f) the employee's hours of employment;

(g) the employee's salary or wages;

(h) the employee's membership of a professional or trade association, including the employee's trade union membership;

(i) the employee's recreation, long service, sick, personal, maternity, paternity or other leave; and/or

(j) the employee's taxation, banking or superannuation affairs.

NB: This clause 17.5 does not apply to New Zealand.

17.6 **What is a "Permitted Health Situation"?**

Permitted Health Situations are detailed in section 16B of the Australian Privacy Act.

In summary:

A Permitted Health Situation exists in relation to the collection of Health Information about an individual if the information is necessary:

(a) to provide health services to the individual, so long as the collection is required or authorised under Australian law (other than the Australian Privacy Act) or the collection is in accordance with professional confidentiality rules of competent health or medical bodies;

(b) for research or the compilation or analysis of statistics relevant to public health or public safety if:

(i) the purposes cannot be served by collecting de-identified information; and

(ii) it is impracticable to obtain the individual's consent; and

(iii) the collection is required by or under an Australian law or the information is collected in accordance with professional confidentiality rules of competent health or medical bodies; or

(c) for the management, funding or monitoring of a health service if the conditions specified in paragraphs (b)(i),(ii)_ and (iii) are satisfied; or

(d) to provide health services to a patient, where the individual's health information needs to be collected as part of the patient's family, social or medical history that is necessary for providing health services to the patient, and the health information is collected from the patient or, if the patient is physically or legally incapable of giving the information, from a responsible person for the patient.

A Permitted Health Situation exists in relation to the use or disclosure of Health Information about an individual if:

(a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety and:

(i) it is impracticable to obtain the individual's consent to the use or disclosure; and

(ii) the use or disclosure is carried out in accordance with approved health and medical research guidelines; and

(iii) in the case of disclosure, the company reasonably believes that the recipient will not disclose the information, or personal information derived from that information;

(b) the company has obtained the information in the course of providing a health service to the individual and:

(i) the company reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another person who is a genetic relative of the individual ; and

(ii) the use or disclosure is conducted in accordance with approved health and medical guidelines about handling genetic information; and

(iii) in the case of disclosure, the recipient of the information is a genetic relative of the individual.

(c) the recipient of the information is a responsible person for the individual, and:

(i) the individual is not physically or legally capable of giving consent to the disclosure; and

(ii) the disclosure is necessary to provide appropriate care or treatment of the individual or is made for compassionate reasons.

Collection, use or disclosure of Health Information in a Permitted Health Situation is also subject to other requirements and restrictions as per section 16B of the Australian Privacy Act.

17.7 **What is a "Permitted General Situation"?**

A Permitted General Situation exists in relation to the collection, use or disclosure of Personal Information if:

(a) it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure and the company reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety or any individual or to public health or safety;

(b) the company has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the company's functions or activities has been, is

being or may be engaged in, and the company reasonably believes that the collection, use or disclosure is necessary in order for the company to take appropriate action in relation to the matter;

(c) the company reasonably believes that the collection, use or disclosure is reasonably necessary to assist any entity or person to locate a person who has been reported as missing and the collection, use or disclosure complies with any applicable rules made under the Australian Privacy Act;

(d) the collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim; or

(e) the collection, use or disclosure is reasonably necessary for the purpose of a confidential alternative dispute resolution process.

NB: This clause 17.7 does not apply to New Zealand.