

Introduction

In the performance of its duties, the Northrop Group (Northrop) is required from time to time to collect, hold, use, disclose, and/or dispose of personal information relating to individuals (including but not limited to its customers, contractors, suppliers and employees). Northrop acknowledges that its employees may have access to information that is personal and sometimes also highly confidential regarding Northrop, its employees, and clients.

This Privacy and Confidentiality Policy outlines the practices and procedures implemented by Northrop to ensure the privacy and protection of personal information relating to its employees, clients and suppliers. We are committed to complying with the *Privacy Act 1988* (Cth) (the Privacy Act) and the Australian Privacy Principles (APPs) set out in Schedule 1 of the Privacy Act.

Purpose

The purpose of this policy is to:

- Outline the types of personal information we collect.
- Explain how we collect, use, disclose, and store personal information.
- Detail the rights of employees, clients and suppliers regarding their personal information.
- Ensure compliance with the Privacy Act and the APPs.

Scope

This policy applies to all employees, including full-time, part-time or casual, temporary, fixed-term term or permanent candidates, student placements and trainees, contractors, consultants and third parties engaged by Northrop.

Definitions

Confidentiality - Is the obligation of our employees and third parties to prevent the unauthorised disclosure of personal or sensitive information.

Personal Information - Information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Privacy - Refers to the right of individuals to control their personal information and how it is collected, used, and disclosed.

Sensitive Information - Information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation, criminal record, or health information.

Collection of personal information and sensitive information

Northrop will only collect personal or sensitive information which is reasonably necessary for our functions or activities.

In the process of collecting personal information about an individual, Northrop will take reasonable steps either to notify the individual or to ensure the individual is aware of the data being collected, the purpose for collecting the information, and how it will be used. Methods may be in the form of an electronic message such as email, via other forms such as the Northrop website, a formal employment contract with a section related to data privacy (such as employment terms and conditions) or by provision of this policy.

The information that Northrop collects depends on the relationship the individual has with Northrop. Information collected for our clients and suppliers will differ from information collected for our employees or subcontractors.

Types of Personal Information Collected

We may collect the following types of personal information:

Employees and Job Applicants

- Personal details (e.g., name, address, date of birth, gender, residency status).
- Contact information (e.g., phone number, email address, emergency contacts).
- Qualifications and professional registrations/accreditations
- Employment details (e.g., position, team, work history, references).
- Financial information (e.g., bank account details, tax file number, superannuation account details).

Clients, suppliers, contractors, and consultants:

- Personal details (e.g., name, address, date of birth, gender, licensing and registrations, professional affiliations).
- Contact information (e.g., phone number, email address).
- Business details (e.g., company name, position, ABN).
- Financial information (e.g., bank account details, credit card information, financial status, payment details).
- Project-specific information (e.g., project requirements, specifications).

Methods of Collection

Personal information is collected through:

- Employment application forms.
- Interviews and employment-related meetings.
- Performance reviews and assessments.
- Workplace health and safety records.
- Direct communication (e.g., post, emails, phone calls, meetings).
- Client and supplier registration forms.
- Contracts and agreements.
- Invoices and payment processing.
- Project documentation and correspondence.
- Via access to our website.
- Registration to attend events we host or authorise.
- Registration to receive any of our publications or newsletters.

Sensitive Information

Northrop may collect sensitive information with an individual's consent, or where required or authorised by law, which may include health information (e.g., medical certificates, relevant health conditions).

In rare instances, Northrop may collect sensitive information without an employee's consent if necessary to investigate any suspected serious misconduct or unlawful activity.

Use of Website

Northrop collects data via a "cookie" data files stored on your device when our website is accessed. Our website uses WordPress cookies and Google Analytics cookies.

WordPress cookies collect user authentication details, which are necessary for the website to function properly, and a full list of WordPress cookies can be found at the link: [WordPress Cookie Policy](#).

Google Analytics collects information about access and use of the website and tracks:

- Your country and approximate geolocation.
- Your activity on our website.
- Your IP address (which is anonymised by Google to avoid personal identification and purged once it has been used to determine approximate geolocation).
- Browser and device information.

Links to a full list of default events and user properties collected via Google Analytics are available here:

- [Google Analytics - Automatically collected events](#)
- [Google Analytics - Predefined user dimensions](#)

The information collected via Google Analytics is used to:

- Evaluate the use of the website.
- Compile reports on website activity for us.
- Provide other services relating to website activity and internet usage.

Google may transfer information to third parties where required by law or where third parties process information on behalf of Google. By use of our website, you consent to Google processing data about you – a copy of Google Privacy Policy is available on this link for more information - [Google Privacy Policy](#).

You can opt out of Google Analytics by disabling cookies and JavaScript or using the Google opt-out service available on this link - [Google Analytics Opt-out Browser Add-on Download](#).

Use and disclosure of personal information

Northrop will only use or disclose personal information for the purpose for which it was collected or where there is a legal duty to do so.

Northrop may collect, hold, use, and/or disclose personal information for the following purposes:

- Managing employment relationships.
- Conducting performance evaluations.
- Managing client and supplier relationships.
- Managing and delivering Client services.
- Marketing and business development.
- Business administration, including financial transactions.
- Management and execution of internal projects.
- Training and events.
- Complying with legal and regulatory requirements.
- For the safety of clients, employees, and the general public.
- Auditing and managing the usage of our website.

If Northrop uses personal information for the purpose of direct marketing (where permitted), Northrop will allow an individual to request not to receive direct marketing communications (also known as 'opting out') and will comply with that request.

We may disclose personal information to:

- Regulatory authorities as required by law.
- Our insurers and professional advisors, accountants, business advisors and consultants.
- Third-party service providers (e.g., payroll processors, IT service providers) under strict confidentiality agreements.
- Medical professionals in the event of a workplace injury or health concern.

We may need to provide your personal information to an overseas recipient for example via our cloud based software providers to their team members and affiliates located in Australia, United Kingdom, New Zealand, Singapore, Malaysia, Vietnam and Philippines or to their third party service providers located in EU, USA, Australia, Ireland, UK, NZ, Israel and France.

Our cloud-based software providers are required to enter into written agreements with their third-party service providers requiring them to agree to terms which are compliant with and will remain compliant with applicable law, including the Privacy Act 1988 (Cth).

Storage of personal information

Northrop stores all personal information within electronic systems in a secure centralised database within Australia, with access limited to those representatives of Northrop who need access to the personal information. Northrop takes all reasonable steps to protect personal information from unauthorised or unlawful disclosure.

Northrop will not keep personal data for any longer than is necessary, considering the purpose for which it was first collected, and in line with guidance from our insurers and/or if there is an ongoing query from a statutory body or an ongoing legal claim/court proceeding. Any personal data that is no longer needed may be disposed of securely or de-identified.

Data Breaches Reporting

Any data breach that meets the Notifiable Data Breach Scheme criteria will be reported to the Office of the Australian Information Commissioner (OAIC)

Policy Review

This policy will be reviewed annually by the Privacy Officer or as required to ensure it remains current and compliant with legal and regulatory requirements.

Access and correction of personal data/ complaints

If any person wants to:

- a) know what personal data is held about them;
 - b) access the personal information held about them; or
 - c) correct any data which they believe to be incorrect, incomplete or inaccurate,
- Requests for the relevant action should be made in writing to Northrop's privacy officer.

Northrop may, in some circumstances, refuse to grant access to personal information held, such as where granting access will breach the law, or where Northrop no longer holds the information. If Northrop cannot grant access, we will give written reasons for that decision when we respond to the request to access information.

If you believe that your privacy has been breached, please contact Northrop's privacy officer in writing, providing details of the incident so that Northrop may investigate it. Northrop will investigate your complaint and aim to resolve it within a reasonable time (and any time period prescribed by the Privacy Act). If you do not consider that your complaint has been adequately resolved, you have the right to lodge a complaint with the OAIC via their [privacy complaints process](#).

Northrop's privacy officer for the purposes of the Privacy Act:

Kiri Hetariki

Email address: privacy@northrop.com.au

Telephone number: (02) 9241 4188

Approver
Executive Leadership Team

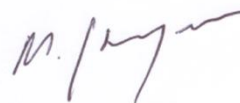
Review Date
April 2025

Document
NCPL44

Revision
03



David Field
Chair



Mark Sturgess
Managing Partner