

Privacy Policy

Last reviewed: April 2026

Our approach

The NTF Group conducts research and analytics for organisations. We aim to collect only the information reasonably needed for each project, explain how identifiable information will be used, separate contact details from research responses where practicable, and report results without identifying participants unless this has been clearly disclosed and authorised.

1. About this policy

The NTF Group Pty Ltd (ABN 60 070 857 279) ("NTF", "we", "us" or "our") is an Australian insights, analytics and research consultancy. We conduct business-to-business (B2B) and business-to-consumer (B2C) research for commercial, government and not-for-profit clients. The Principals of The NTF Group are members of the Australian Market and Social Research Society and abide by its privacy obligations.

This policy explains how we collect, hold, use and disclose personal information across our research, analytics and related business activities. It applies to research participants and subjects; customers, members, employees and stakeholders of our clients; client and supplier contacts; website visitors; and other people whose personal information we handle.

A project-specific collection notice, invitation, consent form or participant information statement may provide additional details. Where it does, that information should be read with this policy. The project-specific notice governs the particular collection to the extent it is more specific and consistent with applicable law.

This policy does not cover high-risk research involving children, health information, biometrics, covert observation, vulnerable participants, or information that could materially affect a person's rights or interests. NTF will obtain project-specific advice and prepare appropriate privacy and participant documentation before undertaking such research.

2. Our role in a research project

Our role varies. In some projects, NTF determines how personal information will be collected and handled. In others, we handle information for a client under its instructions and contractual requirements. We may also work with survey platforms, participant panels, recruiters, interviewers, transcription providers, analysts and other service providers.

When a client supplies contact details or other personal information, we require the client to have appropriate authority to provide it and to tell us any restrictions that apply. We use client-supplied information only for the agreed research or related project purposes, unless another use is required or authorised by law.

3. What personal information we may collect

Depending on the project, we may collect or receive:

Contact and sample information, such as name, email address, telephone number, postal address, customer or member number, employer, job title, organisation, industry and location.

B2B professional information, including a person's role, responsibilities, organisation size, purchasing authority, business needs and professional opinions. Business contact details can still be personal information where they identify an individual.

Research responses, including survey answers, interview and focus-group comments, preferences, ratings, experiences, opinions, complaints, images, documents and other material a participant provides.

Research administration information, such as invitation source, unique survey token, participation or completion status, contact history, consent records, quality-control flags, incentive eligibility and requests not to be re-contacted.

Technical information generated through online systems, which may include IP address, browser and device information, approximate location, timestamps, cookies, log data and interaction data.

Information supplied by a client for analysis, such as customer, transaction, operational, service, complaint, employee or stakeholder information, where this is relevant to the project.

Derived information, such as segments, classifications, model scores, themes and other analytical outputs inferred from research responses or client data.

Business and administrative information about client, supplier and professional contacts, including communications, contracts, invoices and payment records.

Sensitive information

Some research may involve sensitive information, such as health information, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, trade-union membership, criminal history or biometric information. We will only collect sensitive information where it is reasonably necessary for the research or another legitimate function and where the person has consented, or collection is otherwise permitted by law. A project notice will provide additional information where sensitive information is requested.

Please avoid including sensitive or identifying information about yourself or another person in open-text responses unless the question asks for it and you are comfortable providing it.

4. How we collect personal information

We may collect personal information:

- directly from a person through an online, telephone, paper or face-to-face survey; interview; focus group; workshop; observation; diary; usability test; submission; enquiry or other research activity;
- from a client that has engaged us, including from a client-supplied customer, member, employee, broker, supplier or stakeholder list;
- from research panels, specialist recruiters, industry associations, sample providers, fieldwork partners and other research suppliers;

- from publicly available professional and business sources where lawful and appropriate, such as company websites, professional directories, public registers and professional networking profiles;
- through survey, website, communications and security technologies that automatically record technical or interaction information; and
- from another person participating in research, where the project requires information about household members, colleagues, customers or other research subjects and the collection is lawful and reasonable.

Where we collect personal information from someone other than the individual, we will take reasonable steps to ensure the individual is aware of the relevant collection matters, unless an exception applies.

5. Why we collect and use personal information

We may collect, hold, use and disclose personal information to:

- design, recruit for, administer and conduct research and analytics projects;
- contact potential participants, verify eligibility, arrange appointments and send appropriate reminders;
- issue unique survey links, prevent duplicate responses, monitor response quality and manage participation or completion status;
- pay or deliver an incentive and maintain related administrative records;
- analyse responses and data, identify themes and patterns, prepare models and produce reports, presentations, dashboards, data files or other research outputs;
- conduct follow-up research where this has been notified or authorised;
- manage research contact frequency and honour opt-out or do-not-recontact requests;
- meet client contracts, quality assurance, audit, legal and regulatory requirements;
- operate, secure and improve our systems, methods and services; and
- manage our relationships with clients, suppliers and professional contacts.

We do not use identifiable research information to market goods or services to research participants. We may separately send business communications to existing or prospective client contacts where permitted by law, with an appropriate means to opt out.

6. Collection notices, choice and consent

At or before collection, we will ordinarily provide a concise project-specific notice explaining matters relevant to that research. Depending on the project, this may include who commissioned the research, where contact details came from, what information is collected, why it is needed, whether participation is anonymous, confidential or identified, who will receive the information, likely overseas processing and how to contact us.

Participation in our research is generally voluntary. A person may decline to answer a question or stop participating, subject to any practical consequences explained at the time. Where practicable, a participant may ask us to withdraw identifiable material before it has been de-identified, combined with other responses or included in a final output. Once information

has been irreversibly de-identified or included in aggregated findings, we may no longer be able to isolate or remove it.

Where practicable, people may participate anonymously or using a pseudonym. Identification may be necessary for some projects, such as eligibility verification, incentive payment, longitudinal research, response-status tracking or investigation of a particular service experience. We will not collect more identifying information than is reasonably required.

7. Anonymous, confidential and identified research

These terms have different meanings and we use them carefully:

Term	What it means
Anonymous	NTF cannot reasonably identify the participant from the information held. A survey is not anonymous merely because a name is not asked. Unique links, tokens, IP addresses, detailed verbatim comments or a combination of answers may make a person reasonably identifiable.
Confidential	NTF may know or be able to determine the participant's identity, but restricts access and ordinarily reports results in aggregated or de-identified form.
Identified	The participant's identity or identifiable response may be provided to the client or another recipient. This will ordinarily occur only where it has been clearly disclosed and the participant has consented, where it is necessary for the stated purpose, or where it is required or authorised by law.

Before providing verbatim comments to a client, we take reasonable steps appropriate to the project to remove unnecessary identifiers or warn participants that their words may identify them. We may edit a comment to remove identifying details while preserving its substantive meaning.

8. Client-supplied lists, unique links and response status

A client may provide NTF with customer or stakeholder contact information so we can invite people to research. We seek to limit the file to information needed for recruitment and administration, keep it separate from research responses where practicable, restrict access, and delete or return it when it is no longer required.

Some surveys use individual links or pseudonymous tokens. These can help prevent duplicate responses and allow reminders to be sent only to people who have not completed the survey. Unless the relevant notice says otherwise, the client may receive a person's participation or completion status for research administration, but not responses linked to that status. If the client will receive identifiable answers or verbatim comments, this will be clearly disclosed.

9. Disclosure of personal information

We may disclose personal information, where reasonably necessary, to:

- the client that commissioned the project, in the form and on the basis explained to participants;
- survey, panel, recruitment, fieldwork, interview, transcription, translation, incentive and research-quality providers;
- cloud hosting, data storage, communications, collaboration, analytics, visualisation, automation, cybersecurity and IT support providers;
- professional advisers, insurers and auditors; and
- regulators, courts, tribunals, law-enforcement bodies or other persons where required or authorised by law.

We seek to provide service providers with only the information reasonably needed for their task and use contractual, access and security controls appropriate to the nature of the information. We do not sell research participants' personal information.

10. Analytics, artificial intelligence and automated tools

NTF may use statistical modelling, machine learning, natural-language processing and AI-assisted tools to code, classify, summarise or analyse research material. Where an external tool is used, we seek to minimise or remove direct identifiers, select suitable privacy and security settings, restrict provider use of the data, and review material outputs before relying on them.

NTF does not collect or use personal information for automated decision-making. Our research analysis produces insights for clients; no computer program is used to make a decision that could reasonably be expected to significantly affect an individual's rights or interests.

11. Australian data hosting and overseas disclosure

All data collected through NTF survey platforms and other NTF operational platforms is stored on systems based in Australia.

NTF does not ordinarily disclose identifiable research information to overseas recipients. If a project requires overseas storage, access or disclosure, NTF will assess the arrangement before it occurs, take the steps required by Australian privacy law, and provide additional notice or obtain consent where required. The project may be governed by a separate or supplementary privacy notice.

12. Data security

We take reasonable technical and organisational steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. Depending on the information and project, these measures may include:

- role-based access and least-privilege controls;
- multi-factor authentication and strong account-management practices;
- encryption in transit and, where available and appropriate, at rest;
- secure file-transfer methods and restrictions on sending personal information by ordinary email;
- separation of contact or token files from response data where practicable;

- data minimisation, de-identification and suppression of unnecessary identifiers;
- contractual confidentiality and security requirements for personnel and suppliers;
- system monitoring, backups, patching and incident-response procedures; and
- staff awareness and review of privacy and security requirements.

No method of electronic transmission or storage is completely secure. If we become aware of a suspected data breach, we will investigate, contain and assess it and will notify affected individuals, clients and the Office of the Australian Information Commissioner where required.

13. Retention and destruction

We retain personal information only for as long as reasonably needed for the project, the purposes described in this policy or a collection notice, contractual obligations, quality assurance, dispute management, legal requirements and legitimate recordkeeping.

Unless a contract, collection notice or law requires another period, our general practice is to delete or de-identify direct identifiers, client-supplied sample files and other raw identifiable research material within 6 months after the final project deliverable. A shorter period may apply to contact lists and survey tokens. Administrative, consent, financial and contractual records may be kept for longer where required, commonly up to seven years. De-identified research data and aggregated outputs may be retained for research, methodological, benchmarking and recordkeeping purposes because they are no longer personal information.

We may retain minimal suppression information, such as an email address or telephone number, where necessary to honour a request not to be contacted again. When information is no longer required, we take reasonable steps to securely delete, destroy or de-identify it, subject to backup cycles and lawful retention requirements.

14. Access and correction

A person may ask whether we hold personal information about them and request access to, or correction of, that information. Requests should be sent to the Privacy Officer using the details below. We may need to verify identity before responding.

We will respond within a reasonable period, ordinarily within 30 days. We generally do not charge for making a request, although we may charge a reasonable amount for providing access where permitted. Privacy law may allow or require us to refuse access in some circumstances. If we refuse a request, we will ordinarily explain why and describe available complaint options.

Access may be limited where information has been de-identified or aggregated so that NTF can no longer identify the individual, or where providing access would unreasonably affect another person's privacy or reveal commercially sensitive material.

15. High-risk projects

This policy does not cover high-risk projects involving children, health information, biometrics, covert observation, vulnerable participants, or information that could materially affect a person's rights or interests. Before undertaking such a project, NTF will obtain project-specific privacy or legal advice, assess the risks, and prepare any tailored consent, participant information and privacy documentation required for that project.

16. Websites, cookies and online services

NTF websites, including ntfgroup.net, ntf.com.au and any other NTF website, do not use analytics, advertising cookies, enquiry forms or embedded third-party content.

To the extent that basic technical or security logs are automatically generated by a website host, they are stored in Australia and used only to operate, maintain and protect the website. Links to third-party websites are provided for convenience. We are not responsible for the privacy practices of websites or services we do not control.

17. Privacy complaints

A person who believes we have mishandled personal information may contact our Privacy Officer. Please describe the concern and provide any information that will help us investigate. We aim to acknowledge a complaint promptly and provide a substantive response within 30 days, although complex matters may take longer. We will explain any delay.

If the person is not satisfied with our response, they may be able to complain to the Office of the Australian Information Commissioner (OAIC). The OAIC generally expects a person to raise the matter with the organisation first and allow a reasonable time for a response. More information is available at www.oaic.gov.au/privacy/privacy-complaints or by calling 1300 363 992.

18. Changes to this policy

We may update this policy to reflect changes in law, research methods, technology, service providers or our information-handling practices. The current version will state its effective date and last review date. Material changes will be communicated where reasonable and appropriate.

19. Contact us

Privacy Officer

The NTF Group Pty Ltd

ABN 60 070 857 279

Email: admin@ntf.com.au

Location: 1 Sussex Street, Barangaroo, Sydney NSW 2000, Australia

Project enquiries

For a question about a particular survey, interview or other research activity, please include the project or client name shown in the invitation or collection notice. This helps us locate the correct records without asking for unnecessary personal information.