Privacy and confidentiality guidelines
Crown copyright ©
See Copyright and terms of use for our copyright, attribution, and liability statements.

Citation

ISBN 978-0-9941463-1-1 (online)

Published in May 2017 by
Stats NZ Tatauranga Aotearoa
Wellington, New Zealand

Contact
Stats NZ Information Centre. info@stats.govt.nz
Phone toll-free 0508 525 525
Phone international +64 4 931 4600

www.stats.govt.nz
Contents

Context ........................................................................................................................................... 4

Key considerations when dealing with personal and confidential information ....................... 4

How the Privacy Act and Statistics Act apply to all personal and confidential information .... 5

  Differences between the Privacy Act and the Statistics Act relating to personal information ........................................................................................................ 5

  Summary of how Privacy Act information privacy principles apply to personal information ........................................................................................................ 6

Guidance for applying Privacy Act information privacy principles and the Statistics Act ...... 7

  Only collect information that is relevant and necessary (IPP1) ............................................. 7

  Collect information directly from the individual wherever possible (IPP2) ......................... 7

  Be open about the intended use of confidential information (IPP3) ..................................... 8

  Be fair and respectful in the way you collect confidential information (IPP4) .................... 8

  People have a right to access and correct personal information (IPP6 & 7) ...................... 8

  We check confidential information for accuracy before we use it (IPP8) ......................... 9

  Only retain confidential information for as long as it is needed (IPP9) ............................... 9

  Confidential information may be used for other purposes (IPP 10) ................................. 9

  Confidential information will not be disclosed without authorisation (IPP11) ................. 10

  Assign randomised Stats NZ unique identifiers – not identifiers used by other organisations (IPP12) ......................................................................................... 10

Definitions .................................................................................................................................. 10

Responsibilities .......................................................................................................................... 12

Related documents ...................................................................................................................... 14

  Guidelines and procedures .................................................................................................... 14

  Other documents ................................................................................................................... 15

  Legislation .............................................................................................................................. 15

Owner and review ....................................................................................................................... 15
Context

Stats NZ staff, secondees, and contractors use Privacy and confidentiality guidelines to apply the Information privacy, security and confidentiality policy to the management of personal and other confidential information of respondents, staff, customers, and other people and organisations we deal with.

Willingness by these groups to provide us with information is central to our work and is enabled by the high level of trust and confidence in the way we secure this information. To maintain this critical level of trust and confidence we must be mindful of expectations about privacy, security, and confidentiality. We are committed to ensuring our policies and processes for the collection, use, storage, security, and disposal of personal and other confidential information, and the technology we use to support our processes, not only comply with all relevant legislation and statistical principles and protocols, but also meet public expectations, and are effectively implemented.

At the same time we aim to get maximum benefit from the information we manage. To achieve this, information should be open and access to it restricted only where necessary. We should share information as freely as legislation permits, while at the same time carefully considering public expectations, commitments made at the time of collection about how the information would be used, and always endeavouring to protect against potential harm.

You might also be interested in our policy and guidelines aimed at protecting against the potential harm posed from the most at-risk data we hold:

- Information privacy, security, and confidentiality policy
- Data integration guidelines
- Microdata access guidelines.

Key considerations when dealing with personal and confidential information

Stats NZ staff who deal with personal and confidential information must take into consideration the following points:

1. Think about privacy and confidentiality issues at the start of any project to develop or change any Stats NZ's system or process.
2. Think about privacy and confidentiality risks as an integral part of our risk management framework and processes. Use the Privacy & Confidentiality Impact Assessment Guidance and related templates, available from the senior advisor, Strategy Performance and Privacy.
3. Breach and incident management and reporting are handled through Stats NZ's senior advisor, strategy, performance and privacy and the security team. If a breach or incident occurs, the first steps are to attempt to recover the information, contain the breach, minimise harm, and notify the responsible manager; senior advisor, strategy, performance and privacy; and security manager (using the intranet security/privacy incident reporting tool under ‘useful links’ on Te Matapihi).
How the Privacy Act and Statistics Act apply to all personal and confidential information

At Stats NZ, we deal with personal information from three categories of people:
- respondents
- staff
- customers and stakeholders.

The 12 information privacy principles of the Privacy Act 1993 apply to all three categories, but the Statistics Act 1975 only applies to the survey respondents’ personal and confidential information.

The purpose of the Privacy Act 1993 is to protect the privacy of individuals, which it does by a principles-based approach. Some of the information privacy principles contain exemptions for when information is used for statistical or research purposes. The intent behind the Privacy Act’s principles is applicable to all types of information under our care and therefore provides useful guidance for both personal and other confidential information management.

Differences between the Privacy Act and the Statistics Act relating to personal information

**Respondent information**

This is personal information about individual respondents, collected under the authority of the Statistics Act 1975.

**Privacy Act:** Apply all 12 information privacy principles, unless you can use exemptions relating to statistical and research use. See Privacy Act information privacy principles 2, 3, 6, 7, 10, 11, and section 7(2) and 7(5).

**Statistics Act:** You can only use respondent information for statistical or research purposes. You need to apply appropriate confidentialisation and/or de-identification procedures to protect against unauthorised disclosure of personal information by any reasonably foreseeable means.

**Staff information**

This is personal information about individual employees or prospective employees.

**Privacy Act:** Apply all 12 information privacy principles.

**Statistics Act:** Not applicable.

**Customer and other information**

This is personal information about individual customers or stakeholders.

**Privacy Act:** Apply all 12 information privacy principles.

**Statistics Act:** Not applicable
Summary of how Privacy Act information privacy principles apply to personal information

Follow this summary of how to apply information privacy principles (IPPs) when you deal with personal information. These guidelines are also applicable to confidential information about households, iwi, and organisations and therefore can be used to guide decisions about management of all confidential information.

**Principle 1: Purpose of collection of personal information (IIP1)**
Only collect information Stats NZ really needs.

**Principle 2: Source of personal information (IPP2)**
Get information directly when possible.

**Principle 3: Collection of information from subject (IPP3)**
Be open with people about how we are going to use their information.

**Principle 4: Manner of collection of personal information (IPP4)**
Be fair about how we get information.

**Principle 5: Storage and security of personal information (IPP5)**
Keep information secure.

**Principle 6: Access to personal information (IPP6)**
Let the person see their information if they want to.

**Principle 7: Correction of personal information (IPP7)**
When appropriate, correct information if requested to do so.

**Principle 8: Accuracy of personal information to be checked before use (IPP8)**
Where appropriate and practical, check information is fit for purpose before using it.

**Principle 9: Organisation not to keep personal information for longer than necessary (IPP9)**
Dispose of information securely if it is no longer needed.

**Principle 10: Limits on use of personal information (IPP10)**
Use information only for the purpose we got it.

**Principle 11: Limits on disclosure of personal information (IPP11)**
Only disclose information if we have authorisation and the reason is justified.

**Principle 12: Unique identifiers (IPP12)**
Do not use unique identifiers if prohibited by the Privacy Act.
Guidance for applying Privacy Act information privacy principles and the Statistics Act

Here is more detail on how we fulfil our obligations to the information privacy principles (IPPs) in the Privacy Act, and our responsibilities under the Statistics Act.

These processes apply to how we manage information about people, households, and organisations.

Only collect information that is relevant and necessary (IPP1)

Respondent information
The Government Statistician is authorised under the Statistics Act to collect information for statistical or research purposes. We only collect information, under this authorisation, if it adds value to New Zealand when it is used for statistical or research purposes.

Staff information
When we collect information about staff, we only collect information that is necessary and relevant for the purpose of recruiting, selecting, and managing people.

Other personal or organisation information
We collect information relating to customers in a number of ways, for example, when we consider requests to access research data, interact with people via our website, compile information for marketing or consultation purposes, or provide guests with access to the internet via guest Wi-Fi. In all cases we should ensure we only collect the minimum information necessary.

Collect information directly from the individual wherever possible (IPP2)
We collect information directly when we conduct statistical surveys. Occasionally we need to collect from a related person (for example, someone who can help if a disabled people is not able to respond directly). The Privacy Act enables collection of personal information from other organisations, provided it is only used for statistical or research purposes.

We collect information from other organisations and integrate it with other datasets to produce official statistics and for research purposes. We protect against disclosure of confidential information by de-identification and confidentialisation. Furthermore, data is only made available to organisations and researchers who have agreed to our strict disclosure protection requirements, undertaken training, and signed our declaration of secrecy. A privacy and confidentiality impact assessment is required for all data integration proposals (see Data integration policy guidelines). Approval is granted if there are significant benefits to New Zealand and risks can be appropriately mitigated. Additional checks are also made by Stats NZ staff and systems prior to release of any outputs.
When we collect confidential information in other contexts, such as recruitment or customer interactions, we collect it directly from the person or organisation concerned, or with their agreement, from others such as referees.

**Be open about the intended use of confidential information (IPP3)**

The Privacy Act principles require openness with people about how the personal information we collect will be used. The Principles and Protocols for Producers of Tier 1 Statistic also require people to be informed of the main intended uses of the information they are required to provide.

While it is not possible to predict details of uses unrelated to the original purpose of collection, we explain the potential use for unrelated statistical and research purposes. We also ask other organisations that collect confidential information to inform people that the information they provide may be integrated with other data sources for statistical or research purposes.

We also collect confidential information from staff, customers, or other people we interact with. For example, we collect confidential information:

- from prospective staff members to facilitate the recruitment process
- from staff members to facilitate pay, leave, or other staff management processes
- about customers or stakeholders in order to better understand their needs.

In all cases we make the person aware what information is being collected, why it is being collected, and how it will be used.

**Be fair and respectful in the way you collect confidential information (IPP4)**

We should be mindful that collecting confidential information involves a degree of intrusion into people’s lives, and hence we approach it in a respectful manner. We consider people’s views on sensitivity of information we propose to collect, and any special characteristics of the group of people or organisations we are proposing to collect from. We minimise the intrusiveness when we collect information.

**We protect confidential information (IPP5)**

Our security policies and procedures ensure confidential information will be stored securely, and disclosure restricted to approved users and for authorised uses. Our staff should only have access to confidential information when required for their role.

**People have a right to access and correct personal information (IPP6 & 7)**

Customers, current, and former staff, and other people we deal with have a right to access and correct information we hold about them.

Although the Privacy Act requirement to provide respondents access to the information they supplied does not apply directly to Stats NZ, the Statistics Act gives the Government Statistician the discretion to agree to such requests.
Our policy is to agree to requests by respondents (a person or organisation) for access to confidential information about themselves, provided the information is readily retrievable, and we can be certain it is information that belongs to them. This aligns with the Privacy Act and our desire to be transparent and maintain people’s trust in us.

It may be difficult to access confidential information, depending on when it was collected and the collection method. For example, when we integrate data from different sources, de-identification processes make it difficult to retrieve information specific to a person or organisation. However, the source agency supplying the data to us should be able to retrieve the data more easily and in those cases we will transfer the information request to that agency.

We verify the requestors’ identity before we grant access. If the information was collected under the Statistics Act, the request is authorised by the Government Statistician. All requests for access to confidential information are referred to the senior advisor, strategy, performance and privacy.

We deal with requests for access to information about people other than the requestor under the Official Information Act. We have appropriate policies and procedures to ensure privacy protection when we release information under the Official Information Act.

**We check confidential information for accuracy before we use it (IPP8)**

We make reasonable efforts, appropriate to the intended use, to ensure administrative data collected under the Statistics Act is fit for purpose before we use it. Other confidential information held by Stats NZ should be regularly reviewed to ensure it is accurate before we use it. For example, stakeholder databases should be checked for accuracy before they are used.

We encourage Stats NZ staff to check information we hold on them in our leave management system, so we can keep it up to date.

**Only retain confidential information for as long as it is needed (IPP9)**

We do not retain confidential information beyond its original purpose, unless there is long-term statistical or research value in doing so. We retain data that has long-term statistical or research value so it can continue to be used to benefit New Zealand.

We apply the Information and data management policy (Statistics NZ, 2013) to all information we hold, including data, metadata, census schedules, staff information, and financial records. Retention, preservation, and disposal of information, including confidential information, is managed by Information Management and requires appropriate approvals.

**Confidential information may be used for other purposes (IPP 10)**

An exemption in the Privacy Act enables Stats NZ to use personal information for statistical and research purposes (provided individuals can not be identified) even when it was collected for another purpose. This also applies to information provided to us by other organisations.

Apart from statistical and research purposes, we do not use confidential information we collect for any purpose unrelated to the purpose it was collected for, unless permission is obtained from the
individual or organisation concerned. We are committed to making information available about how we are going to use information we collect.

Confidential information will not be disclosed without authorisation (IPP11)

Under the Statistics Act, we do not disclose respondents’ information outside Stats NZ without the consent of the respondent. However, with the approval of the Government Statistician, we make de-identified information available to approved researchers, for approved research purposes, in secure environments (see for example Microdata access guidelines).

We do not disclose other confidential information, unless the disclosure is part of the purpose it was collected for. For example, a manager would need to be able to see personal information about a staff member for the purposes of staff management. But we do not pass information about a staff member to someone outside Stats NZ without that staff member’s permission.

Assign randomised Stats NZ unique identifiers – not identifiers used by other organisations (IPP12)

Unique identifiers include such things as IRD numbers, NHI/national health index numbers, bank client numbers, driver’s licence, and passport numbers.

For statistical and research purposes, we use encrypted unique identifiers assigned by other organisations, such as tax numbers, for longitudinal linking (surveys repeated over time), and data integration.

Some unique identifiers, such as the New Zealand business number, are specifically intended to be used by multiple organisations and should be used where possible. Other unique identifiers assigned by other organisations should only be kept if needed for ongoing longitudinal linking or data integration. If retained, we keep them separately from data used for analysis and research, and we restrict access (see Data integration policy guidelines).

We remove all identifying information, including unique identifier assigned by original organisation, from data used for statistical and research purposes, and we replace the unique identifier assigned by the original organisation with a Stats NZ randomised unique identifier.

When dealing with staff, customers, other organisations, and people other than respondents, you may assign unique identifiers where necessary to efficiently carry out our business activities. An employee number is an example of a unique identifier used by Stats NZ. This is necessary to enable our employee databases to operate.

Definitions

anonymised

Term most commonly used to refer to data from which direct identifiers have been removed (de-identified data) but is sometimes used to refer to confidentialised data. It is not a term used in these guidelines.
availability
Ensuring authorised users, including staff, contractors, and researchers, can access data and information for authorised purposes at the time they need to do so.

confidential information
Data and information about a person, household, iwi, or organisation that we should not disclose to people who are not authorised to have access to it. Confidential information may be obtained from respondents, other organisations, customers, staff, or other people we deal with. Confidential information also includes embargoed releases and Stats NZ operational information that is not already publicly available.

Note: ‘confidential’ is a classification used by the New Zealand Government in its classification system for information pertaining to national security. Stats NZ does not hold or store any information classified confidential or any other information pertaining to national security, therefore we use the common English definition of confidential. For further information about the government information classification system, see Protective Security Requirements.

confidentialisation
The statistical methods used to protect against confidential information being disclosed to people who are not authorised to have access to it, in a way that could identify an individual, household or organisation. The statistical methods used provide a level of protection against identification that cannot be obtained from de-identification.

confidentiality
The protection of information provided by people and organisations to us and ensuring it is not disclosed or made available to people or organisations who are not authorised to access it. Authorisation should ideally be given by the person providing the information, but may also be through legislation.

data integration
The linking of data about the same person or organisation (or unit) from two or more unit record datasets, originally collected for different purposes.

de-identification
The process of removing information from microdata to reduce risk of spontaneous recognition. It typically includes removing names, exact dates of birth or death, and exact addresses.

information security
The measures put in place to protect against data and information being disclosed to unauthorised people or organisations, and to ensure appropriate availability and integrity of information.

Integrated Data Infrastructure (IDI)
Database containing de-identified people-centred microdata from a range of government agencies, Stats NZ surveys and non-government organisations.

integrity
Assurance about the accuracy and consistency of data and information and that it is authentic and complete. It includes assurance that data and information has been properly created and has not been tampered with, damaged, or subject to accidental or unauthorised changes.
**Longitudinal Business Database (LBD)**
Database containing microdata about businesses from Stats NZ surveys and a range of administrative data sources.

**microdata**
Data about individual people, organisations, households, or other units in a population.

**personal information**
Data and information about a person that we should not disclose to people who are not authorised to have access to it. It is a subset of confidential information.

**privacy**
The individual’s rights relating to control of the provision, use, and disclosure of information about themselves, commonly called their personal information.

## Responsibilities
Here is a summary of who is responsible for what under the privacy and confidentiality guidelines.

**All Stats NZ staff, secondees, and contractors**
- Understand the principles, policies, and procedures relating to the security and management of confidential information.
- Apply these as appropriate to their role.
- Report breaches, incidents, and near misses to the security and privacy teams.

**Chief digital officer**
- Fulfil the role of chief information security officer as defined in the New Zealand Information Security Manual (GCSB, 2016).
- Develop a security strategy and security risk management programme.
- Maintain appropriate security measures to protect the information gathered, stored, and transmitted by Stats NZ.
- Manage and maintain organisation-wide information security policies.
- Manage and maintain certification and accreditation processes.
- Act as an escalation point on security-related matters.

**Chief methodologist**
- Manage and maintain policies and standards relating to statistical confidentialisation.
- Approve confidentialisation and/or de-identification procedures before information is released by subject matter areas.
- Assist in managing confidentialisation-related breaches.
- Provide advice and training to subject matter areas on confidentialisation methods and practice.
- Provide confidentialisation advice to partner organisations.
Chief people officer
- Ensure that staff information is held securely with access limited only to those staff who need access for HR management purposes.
- Ensure privacy and confidentiality policies and guidelines are applied to management of staff information.

Chief privacy officer
- Maintain and manage the information privacy, security, and confidentiality policy, and any other related policies.
- Act as final escalation point on privacy and other confidentiality-related matters.

Chief security officer
- Act as final escalation point on security-related matters.

Deputy Government Statistician
- Approve data integration that only uses data collected directly by Stats NZ.

Government statistician
- Approve data integration proposals and escalated microdata access applications.
- Approve use of any exemptions under clauses 37A to 37F of the Statistics Act 1975 or delegating approval authority.

Information Privacy, Security and Confidentiality (IPSaC) Governance Group
- Provide governance oversight of privacy, security, and confidentiality policies.
- Agree policy implementation work programmes.
- Drive implementation of the work programmes.

Manager and data custodian responsible for releasing data
- Undertake risk assessment, specify risks to be mitigated, and collaborate with Statistical Methods and data specialists to determine appropriate confidentialisation and de-identification techniques. Gain the approval of the Chief Methodologist for application of those techniques.
- Ensure analysts and researchers in their area are trained in how to apply the approved confidentialisation and/or de-identification procedures and that these procedures are applied to information prior to release.

Manager, information management
- Advise and provide education about correct management, retention, and disposal of confidential information in accordance with the Public Records Act 2005 and approved disposal authorisations.

Manager, Integrated Data Infrastructure (IDI) system
- Develop and apply guidelines and processes for data integration in the Integrated Data Infrastructure (IDI) system and assess IDI integrations for approval.

Manager, microdata access
- Develop and apply processes for assessing research and researchers to determine whether researchers and projects should be recommended for approval, and ensure requirements of the Microdata Guidelines are carried out.
Respondent advocate
- Provide a respondent perspective when policies and procedures relating to privacy and confidentiality are developed and implemented.

Security manager
- Fulfil the role of an information technology security manager as defined in the New Zealand Information Security Manual.
- Provide leadership, advice, and consultation on security related issues.
- Manage the implementation of security measures.
- Lead the management of security breaches and incidents.
- Lead security education and awareness activities.

Senior advisor, strategy, performance and privacy
- Design and implement approaches to implement the information privacy, security, and confidentiality policy, including education and awareness activities.
- Lead management of privacy-related breaches and incidents.
- Lead management of confidentiality-related breaches and incidents.
- Provide leadership, advice, and consultation on privacy and confidentiality related issues, including privacy and confidentiality impact assessments.
- Consult with the Office of the Privacy Commissioner when required.

Senior manager, integrated data
- Has delegated authority to disclose individual schedules in the form of de-identified microdata or confidentialised unit record files (CURFs) and to approve variations to existing microdata access approvals.

The Confidentiality Network
- Provide support, advice, and build capability across Statistical Methods, Stats NZ, and the Official Statistics System in confidentiality methodologies and practices.

Related documents

Guidelines and procedures


Other documents


Statistics NZ (nd). Our privacy commitment (poster). Available from Stats NZ, email: info@stats.govt.nz.


Legislation


Owner and review

The director of organisation, strategy and performance is the owner of Privacy and confidentiality guidelines. The 2017 guidelines resulted from a review in 2016, and replace the 2014 Privacy policy (2014). The guidelines will be reviewed annually.