



GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI



New Zealand  
Security Intelligence  
Service  
Te Pā Whakamarumaru

## Joint Policy Statement: JPS - 009

### JPS - Privacy

<b>Policy Owner</b>	Chief Privacy Officer, GCSB Chief Privacy Officer, NZSIS
<b>Policy Administrator</b>	Compliance and Policy Manager, GCSB Compliance and Risk Manager, NZSIS
<b>Approval Authority</b>	Director-General, GCSB Director-General, NZSIS
<b>Approval Date</b>	
<b>Review Date</b>	Three years from signing

## Contents

<b>Purpose</b> .....	3
<b>What is Privacy?</b> .....	3
<b>Background</b> .....	3
<b>Scope</b> .....	4
<b>Definitions</b> .....	5
<b>Relevant legislation/guidance</b> .....	5
<b>Policy</b> .....	7
<b>Privacy officers</b> .....	7
<b>Information Privacy Principles (IPPs)</b> .....	8
<i>IPP 1: purpose of collection of personal information</i> .....	8
<i>IPP 4: manner of collection of personal information</i> .....	8
<i>IPP 5: storage and security of personal information</i> .....	9
<i>IPP 6: access to personal information</i> .....	10
<i>IPP 7: correction of personal information</i> .....	10
<i>IPP 8: accuracy, etc. of personal information to be checked before use or disclosure</i> .....	10
<i>IPP 9: agency not to keep personal information for longer than necessary</i> .....	11
<i>IPP 10: limits on use of personal information</i> .....	11
<i>IPP 11: limits on disclosure of personal information</i> .....	12
<i>IPP 12: Disclosure of personal information outside of New Zealand</i> .....	12
<i>IPP 13: unique identifiers</i> .....	13
<b>Privacy breach and incident management</b> .....	14
<b>Privacy Impact Assessments</b> .....	15
<b>Roles and Responsibilities</b> .....	17
<b>Previous Policy Revoked</b> .....	18
<b>Approvals</b> .....	19
GCSB Approval .....	19
NZSIS Approval .....	19
<i>Effective date and review date</i> .....	19
<b>Summary of Minor Amendments</b> .....	20
<b>Appendix 1 – Privacy Officers</b> .....	21
NZSIS Privacy Officer .....	21
GCSB Privacy Officer .....	21

## Purpose

1. The purpose of this policy is to provide an overview of GCSB's and NZSIS's (the agencies') legal obligations in regard to the law of privacy in New Zealand and to demonstrate the agencies' commitment to good practice in this area.
2. As is required for the agencies to fulfil their statutory functions, GCSB and NZSIS employees have access to various types of personal information not available to other agencies or the public. Such access makes it especially important that GCSB and NZSIS have robust principles and processes for the collection, control and disclosure of personal information.
3. As set out below, the law of privacy in New Zealand is primarily governed by the Privacy Act 2020. The agencies are also subject to the New Zealand Bill of Rights Act 1990 ('NZBORA'), including section 21 which provides individuals with a right to be free from unreasonable search and seizure. In addition to these Acts, there are also two torts (causes of action in the common law) that are relevant to the law of privacy.
4. Respect for privacy is also a consistent theme throughout a number of the Ministerial Policy Statements ('MPS') made under the Intelligence and Security Act 2017 ('ISA'). As such, this policy outlines the principles that apply to the agencies and the considerations that employees must have regard to.

## What is Privacy?

5. Privacy is notoriously difficult to define because it is highly contextual. For example, whether something is considered 'private' varies according to social, political, technological, historical or other factors present, including the relationship of the parties involved and their intention.
6. It is precisely because privacy is so contextual that there is no definition of privacy in the Privacy Act 2020 and no general right to privacy in the New Zealand Bill of Rights Act 1990.

## Background

7. GCSB and NZSIS collect personal information for a range of purposes connected to the statutory functions set out in Part 2 of the Intelligence and Security Act 2017 (ISA). The functions of GCSB and NZSIS are:
  - a. Intelligence collection and analysis;
  - b. Protective security services, advice, and assistance;

- c. Co-operation with other public authorities to facilitate their functions;
  - d. Co-operation with other entities to respond to imminent threat; and
  - e. Any other function conferred or imposed by another enactment.
8. The information the agencies collect is often personal and may be considered private by the individual concerned (i.e. the individual might not publicly disclose the information). The agencies might require the information in order to provide insight into the intentions and views of individuals, enabling GCSB and NZSIS to assess whether they are of intelligence interest or security concern, and carry out their functions under the ISA.
9. GCSB and NZSIS have a number of mechanisms available to them for collecting personal information. Information may be obtained through a declared and overt approach or under a warrant using otherwise unlawful methods such as s6(a) [REDACTED]. Often, the personal information is collected without the consent or knowledge of the individual in question.
10. The collection, management and handling of personal information by GCSB and NZSIS must be in accordance with New Zealand law, including the Privacy Act, and with regard to the principle of respect for privacy in accordance with the relevant MPSs. These principles are outlined within this policy, and are reflected within other agency policy and procedures where relevant.

## Scope

11. This policy applies to all GCSB and NZSIS employees, secondees, s6(a) [REDACTED] and contractors when seeking to collect, use or manage personal information; or where assessing privacy issues and/or impacts in the course of day-to-day work.
12. This policy does not apply to information gathered for human resource purposes. This is provided for in the *JPS - 1.107 Human Resources Information*.
13. This policy does not apply to GCSB and NZSIS's processes for dealing with requests under the Privacy Act. Those processes are covered in agency-specific procedures (*PP-1007 Responding to Information Requests for GCSB and Information Requests Policy for NZSIS*).

<i>Joint Policy Statement - 009</i>	<i>Page: 4 of 21</i>
<i>JPS - Privacy</i>	<i>Version: 1.0</i>
	<i>Date: 1 December 2020</i>

## Definitions

14. The key concepts in this policy are:



- a. **personal information:** information about an identifiable individual;
- b. **IPP:** abbreviation for “information privacy principle”;
- c. **A privacy breach:** in relation to personal information held by an agency
  - (a) means –
    - i. unauthorised or accidental access to, disclosure, alteration, loss or destruction of, the personal information; or
    - ii. an action that prevents the agency from accessing the information on either a temporary or permanent basis; and
  - (b) includes any of the things listed in paragraph (a)(i) or an action under paragraph (a)(ii) whether or not it—
    - i. was caused by a person inside or outside the agency; or
    - ii. is attributable in whole or in part to any action by the agency; or
    - iii. is ongoing.
- d. **Tort:** a civil wrong resulting in potential legal liability – for example negligence;
- e. **Unique identifier** means an identifier:
  - (a) that is assigned to an individual by an agency for the purposes of the operations of the agency; and
  - (b) that uniquely identifies that individual in relation to that agency;— but, for the avoidance of doubt, does not include an individual’s name used to identify that individual.

## Relevant legislation/guidance

### Privacy Act 2020

15. The Privacy Act 2020 is the key piece of legislation governing the protection of personal information. The Privacy Act sets out 13 Information Privacy Principles (IPPs) governing personal information. IPPs 2, 3 and 4b do not apply to GCSB and NZSIS and IPP 12 does not apply when GCSB and NZSIS are exercising their statutory functions. The IPPs that apply to GCSB and NZSIS are summarised within the body of this policy and shown in full in Appendix 1.

## Privacy Codes of Practice

16. It should be noted that while the Privacy Act sets the standards for the collection, use and management of personal information, the Privacy Commissioner may release agency specific codes of practice which impact how these principles apply to information held by certain agencies.
17. In accordance with IPP 11(g), in general agencies may disclose information to GCSB and NZSIS where the disclosing agency believes that the information is necessary for GCSB or NZSIS to perform any of their functions. The exceptions to this, in accordance with the Telecommunication Information Privacy Code 2020 and the Credit Reporting Privacy Code 2020, are:
- a. Telecommunications information cannot be disclosed under IPP 11(g) where the disclosure may be sought in accordance with a business records direction under the ISA.
  - b. s6(a) 
18. GCSB and NZSIS must be aware of these restrictions when requesting information from telecommunications providers s6(a)  Further information on the Privacy Codes can be found on the Privacy Commissioner's website.

## Section 21 New Zealand Bill of Rights Act 1990 (NZBORA)

19. As part of the New Zealand government, the agencies are subject to the New Zealand Bill of Rights Act 1990 (NZBORA). Although the NZBORA does not give a general guarantee of privacy, section 21 of the NZBORA provides that everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.
20. Section 21 focuses on intrusions into reasonable expectations of privacy. A general rule is that a search is unreasonable if the circumstances giving rise to it make the search itself unreasonable or if a search which would otherwise be reasonable is carried out in an unreasonable manner.
21. The particular factual circumstances will determine if a search or seizure was unreasonable. This includes consideration of the subject matter of the search or seizure and the time and place it occurred. For example, while it may be lawful to search a place

under a warrant, it may not necessarily be reasonable to conduct a physical search at 2am if the occupants are home.

22. Obtaining personal information by compulsion (for example under an intelligence warrant) will be considered a “search” and/or “seizure” under section 21 and so must be done in a reasonable manner.

### Torts related to privacy

21. In New Zealand, the courts recognise two torts of invasion of privacy:

- a. public disclosure of private facts, where the publicity given to those facts would be considered highly offensive to a reasonable person (for example revealing someone’s sensitive medical information to the media without their permission); and
- b. Intrusion into seclusion in circumstances where this would be highly offensive to a reasonable person (for example, covertly recording video of a person in the shower (this would also be a criminal offence).

22. Given the nature of the agencies’ activities, it is unlikely that they would be in a position to commit such torts, as they tend not to comment publicly on activities, and any intrusion into seclusion is likely to be done under an intelligence warrant requiring prior justification of the necessity and proportionality of the action. However, staff should consider seeking legal advice in situations where they are disclosing private facts publicly to media <sup>s6(a)</sup>

### Policy

23. GCSB and NZSIS staff must consider the privacy implications of their activities, including in respect of any third parties who may be incidentally affected. This is usually undertaken as part of the requirement to consider proportionality, necessity, and reasonableness. In practice, this is considered as part of existing processes, including when developing warrant applications and operational documentation.

24. GCSB and NZSIS must consider privacy when developing new policies and procedures.

### Privacy officers

25. GCSB and NZSIS must have at least one privacy officer each (section 201 of the Privacy Act). Privacy Officer(s) are responsible for:

- a. encouraging their agency to comply with the IPPs;

- b. dealing with requests made to their agency under the Privacy Act;
  - c. working with the Commissioner in relation to investigations conducted under Part 5 of the Privacy Act in relation to their agency; and
  - d. ensuring their agency complies with the provisions of Privacy Act.
26. The Principal Adviser OIA/Ministerial in the Joint Directors-General Office assists the agencies' Privacy Officer(s) by managing requests made to each agency and liaising with the Commissioner in relation to investigations.
27. If employees have any queries about privacy issues, they should be directed to their line manager in the first instance before raising the query with a Privacy Officer if required. The Privacy Officer(s) will act as the conduit to any other relevant team within their agency in order to resolve the issue. The details of each agency's Privacy Officer(s) are contained within the annex of this policy and will be updated as a minor amendment as required.

### Information Privacy Principles (IPPs)

23. The information privacy principles are set out in section 22 of the Privacy Act 2020. Further information on the information privacy principles can be found on the Privacy Commissioner's website.

#### *IPP 1: purpose of collection of personal information*

*IPP 1 provides that personal information shall not be collected by an agency unless the information is necessary for a lawful purpose connected with a function or activity of the agency.*

28. GCSB and NZSIS must ensure that personal information is collected only where it is considered necessary for the performance of one or more of their function(s). In order to meet this requirement, employees should be able to identify what function(s) they are performing when requesting and/or collecting personal information. GCSB and NZSIS employees should also consider how and why the personal information sought is necessary to enable the performance of that function.

#### *IPP 4: manner of collection of personal information*

*IPP 4 (a) provides that personal information shall not be collected by an agency by unlawful means.*

29. GCSB and NZSIS must only collect information in a manner that is otherwise lawful or that is appropriately authorised in accordance with the ISA. Guidance on whether an



authorisation is required and how it can be obtained is within the *JPS-004 - Applications for Intelligence Warrants and Other Legal Instruments*.

30. GCSB and NZSIS are exempt from IPP 4(b), which states that personal information shall not be collected by means that are unfair or intrude to an unreasonable extent on the personal affairs of the individual concerned. Nevertheless, ongoing consideration should be given to the most appropriate and least intrusive mechanism for collecting the information, alongside operational and technical considerations.

*IPP 5: storage and security of personal information*

*IPP 5 requires agencies to ensure that personal information is protected, by reasonable security safeguards, against loss and misuse; as well as unauthorised access, use, modification, or disclosure.*

31. GCSB and NZSIS have stringent requirements on handling all information due to the covert nature of the agencies' work. Information is stored in a secure manner to protect s6(a) and other sensitive material from unauthorised access.
32. GCSB and NZSIS apply access controls and appropriate safeguards to all information to ensure that only those with the relevant "need-to-know" are given access to information. Where technically possible, attempts to inappropriately access information are monitored across both agencies by s6(a) and agency-specific processes (for example, audits).
33. All personal information held by GCSB and NZSIS shall be held securely and protectively marked as appropriate. Personal information will be classified at least as "in-confidence" or "sensitive" (the privacy classifications), if unauthorised disclosure of the information would not compromise the security of New Zealand, but may compromise the security or interests of individuals. However, personal information collected by GCSB and NZSIS will usually have higher classifications due to the national security implications of the information. All personal information will be stored and handled in compliance with the Protective Security Requirements (PSR).
34. Personal information will be disclosed only where permitted by the Privacy Act, or where any other enactment authorises or requires personal information to be made available. For more information on disclosing personal information, see IPP 10, IPP 11 and IPP 12.

*IPP 6: access to personal information*

*IPP 6 states that individuals are entitled to seek confirmation from agencies whether or not the agency holds their personal information, and obtain access to that information.*

35. Individuals are entitled to ask GCSB and/or NZSIS to confirm whether or not the agencies hold any of their personal information. GCSB or NZSIS must consider each request in accordance with agency-specific procedures on responding to Privacy Act requests (*PP-1007 Responding to Information Requests* for GCSB and *Information Request Policy* for NZSIS). GCSB and NZSIS may also respond to requests by neither confirming nor denying the existence of information if releasing such information would prejudice the security, defence or international relations of New Zealand. This should be done in accordance with *Guidance on NZSIS and GCSB use of "neither confirm nor deny" under section 10 of the OIA or section 32 of the Privacy Act*. Employees should speak to the relevant agency Privacy Officer if they require more information about IPP 6.

*IPP 7: correction of personal information*

*IPP 7 entitles individuals to request the correction of their personal information, and to request that a statement of the correction sought, but not made, be attached to their information.*

36. Individuals are entitled to request the correction of information that GCSB and NZSIS hold about them. GCSB or NZSIS must consider each request in accordance with agency-specific procedures about responding to Privacy Act requests.

37. If GCSB or NZSIS determines that a request to correct information will not be granted (for example, if the agency determines the requested correction is incorrect), the individual may request that a statement of the correction sought but not made be attached to the information. GCSB and NZSIS must comply with any such requests.

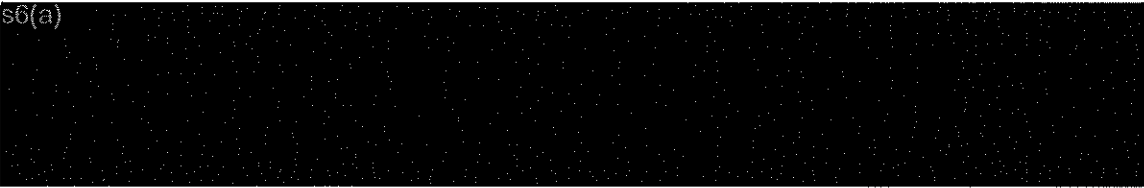
*IPP 8: accuracy, etc. of personal information to be checked before use or disclosure*

*IPP 8 requires agencies to take such steps (if any) as are reasonable in the circumstances to ensure the information it holds, uses, and discloses is accurate, up to date, complete, relevant, and not misleading.*

38. GCSB and NZSIS must take all reasonable steps available to ensure that the information held is accurate, up-to-date, complete and relevant before using or disclosing the information in the performance of any statutory functions.

39. This may include validating the information against other sources of information, and assessing the reliability of the source and any contextual information. The way that

information is assessed and who conducts these assessments will depend on the type of information, the mode of collection and the use of the collected information.

40. s6(a)  


*IPP 9: agency not to keep personal information for longer than necessary*

*IPP 9 states an agency shall not keep personal information for longer than is required for the purpose for which it may lawfully be used.*

41. GCSB and NZSIS must not keep personal information for longer than is required. This obligation must be balanced with the requirement under the Public Records Act 2005, to retain a historical record of the actions and decisions made by the government and its public sector agencies. Direction on the retention of personal information is included within agency-specific data retention and information management policies.

*IPP 10: limits on use of personal information*

*IPP 10 states that personal information collected for one purpose shall not be used for any other purpose unless the agency believes on reasonable grounds that a specified exemption applies.*

42. Any personal information must be collected for a lawful purpose to fulfil a function or activity of the agency, and must only be used for that purpose. In accordance with the specified exemptions, the agencies may, however, use information collected for one purpose for another purpose if they believe on reasonable grounds it is necessary to enable them to perform any of their functions.

43. The ISA also enables GCSB and NZSIS to disclose incidentally obtained information in certain situations. Incidentally obtained information is information that is obtained in the course of performing a function under section 10 or 11 of the ISA but that is not relevant to either of those functions. Incidentally obtained information may be retained for the purpose of disclosure in particular circumstances under section 104 of the ISA. Such information should be identified, handled and shared in accordance with the relevant agency-specific policy and procedures.

*IPP 11: limits on disclosure of personal information*

*IPP 11 states that an agency shall not disclose personal information unless the agency believes on reasonable grounds that a specified exemption applies.*

44. In accordance with the specified exemptions, GCSB and NZSIS can disclose personal information where the agency believes on reasonable grounds disclosure is necessary to enable the agencies to perform any of their functions. One of the functions of the agencies is to collect and analyse intelligence and to share that intelligence and analysis with the Minister responsible for the agencies, the Chief Executive of DPMC and any of the persons authorised by the Minister. This intelligence may include personal information.
45. As well as privacy considerations, GCSB and NZSIS also limit the disclosure of information to protect s6(a). Limiting for one purpose protects the information for the other purpose as well.

*IPP 12: Disclosure of personal information outside of New Zealand*

*IPP 12 states that personal information may only be disclosed to a foreign person or entity with the consent of the individual concerned or if the private information is protected by the Privacy Act or comparable privacy protections.*

46. IPP 12 governs the disclosure of personal information outside of New Zealand. IPP 12 does not apply to information disclosed by GCSB or NZSIS to perform any of the agency's functions.
47. Although IPP 12 often does not apply, GCSB and NZSIS still must have particular regard to the privacy interests of New Zealanders when determining whether to disclose or request personal information from overseas partners in accordance with the MPS on cooperation with overseas agencies.
48. Before sharing any personal information of New Zealanders with an overseas public authority, GCSB and NZSIS must be satisfied that the overseas public authority has adequate protections in place for the use and storage of New Zealanders' information, including adequate protections against further sharing with third parties without express consent from GCSB or NZSIS. For example, appropriately secure communications and storage facilities.
49. When sharing personal information, GCSB and NZSIS must specify the protection, storage and use requirements that are to be adhered to in respect of any information, including personal information about New Zealanders, shared with an overseas public

authority. This may include the classification and dissemination markings of the information and any minimisation processes. Information can only be shared consistently with the principles in the MPS on cooperating with an overseas public authority and the MPS on the management of information.

50. All sharing of information must also be in accordance with Ministerial authorisations and the JPS 006 – Human Rights Risk Management Policy, as well as any other agency-specific policies or Memoranda Of Understanding that govern sharing information (for example s6(a)).

51. If staff members have any queries, requests or proposals for sharing information that raises unfamiliar issues, they should discuss it with their manager and seek advice from the Privacy Officers and the relevant Legal team if necessary. Depending on the issue, other teams may need to be involved s6(a).

*IPP 13: unique identifiers*

*IPP 13 states that an agency shall not assign a unique identifier to an individual unless it is necessary to enable the agency to carry out its functions efficiently. There are specific conditions which apply to unique identifiers.*

52. In certain circumstances, GCSB and NZSIS may assign unique identifiers to individuals in accordance with IPP 13 where it is necessary to carry out their functions efficiently.

s6(a)  
53. [Redacted]

54. s6(a) [Redacted]

55. GCSB and NZSIS staff should speak to the Privacy Officers if they intend to use unique identifiers for individuals for any other purpose. s6(a)

Joint Policy Statement - 009	Page: 13 of 21
IPS - Privacy	Version: 1.0
	Date: 1 December 2020

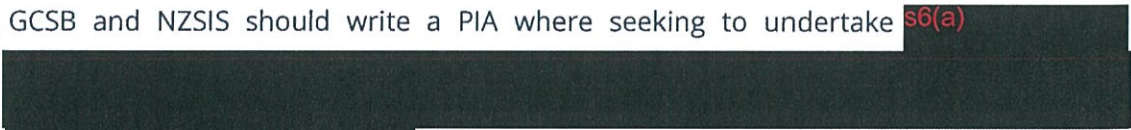
## Privacy breach and incident management

56. If a staff member becomes aware that a privacy breach has, or may have occurred, they must immediately inform their manager who must inform the relevant Compliance team as soon as possible. The Compliance team will inform the agency Privacy Officer(s); and, as appropriate, the Legal team, the <sup>s6(a)</sup> [REDACTED] and other relevant teams.
57. If it is assessed that the privacy breach has likely caused serious harm to an affected individual or individuals or is likely to do so then the Privacy Commissioner must be notified of the breach as soon as practicable.
58. The Privacy Act provides the affected individual must also be notified unless we consider that notification would:
- prejudice security, defence or international relations of New Zealand;
  - prejudice the maintenance of the law;
  - endanger the safety of any person; or
  - reveal a trade secret.
59. The affected individual does not need to be notified if they are under 16 or it could prejudice their health. In these cases a representative may be notified instead.
60. When assessing whether or not a breach is likely to cause serious harm the agencies must consider the following:
- Any action taken by the agency to reduce the risk of harm following the breach
  - Whether the personal information is sensitive in nature
  - The nature of the harm that may be caused to the affected individuals
  - The person or body that has obtained or may obtain personal information as a result of the breach (if known)
  - Whether the personal information is protected by a security measure
  - Any other relevant matters
61. The Compliance team, in cooperation with the Privacy Officer(s), will:
- Attempt to contain the breach and perform an initial investigation;
  - Inform the Inspector-General of Intelligence and Security, if required by the relevant Compliance Framework;

- c. Either notify the affected individual/s or record the reasons why the individual/s were not notified, after considering any security implications;
  - d. Consider whether there has been a notifiable privacy breach and therefore if the Privacy Commissioner must be notified. Any reporting to the Privacy Commissioner or affected individuals will require the Director-General to be briefed; and
  - e. Report to SLT on the breach, where required in accordance with the relevant Compliance Framework.
62. Following a breach, Compliance, in consultation with the Privacy Officer(s) will work with the relevant section(s) of GCSB and NZSIS to assess the effectiveness of current prevention measures to ensure personal information is obtained, used and managed according to the IPPs and this policy. This may require the development and implementation of further prevention strategies.

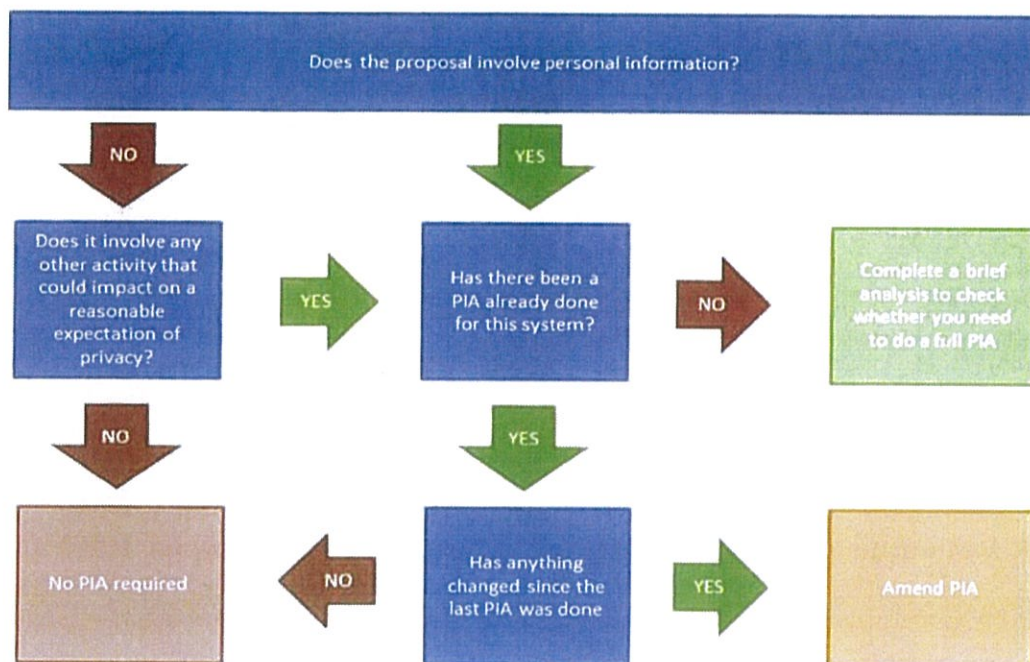
### Privacy Impact Assessments

63. Privacy Impact Assessments ("PIA's") are used by government agencies to identify whether a proposed project is likely to impact on the privacy of individuals affected by, or subject to the project.
64. The Privacy Commissioner's guidance (available on their website) suggests the use of a PIA in instances where a project:
- a. Involves personal information;
  - b. Involves information that may identify individuals;
  - c. May result in surveillance of individuals, or intrusions into their personal space or bodily privacy; or
  - d. May otherwise affect whether people's reasonable expectations of privacy are met.
65. GCSB and NZSIS should write a PIA where seeking to undertake s6(a)



A full PIA should only be completed if a brief privacy analysis suggests we should. If there is an existing PIA it should be amended if there are any significant changes.

<i>Joint Policy Statement - 009</i>	<i>Page: 15 of 21</i>
<i>JPS - Privacy</i>	<i>Version: 1.0</i>
	<i>Date: 1 December 2020</i>



66. The MPS on information assurance and cybersecurity activities requires GCSB to conduct a PIA when developing significant new projects or cybersecurity activities that have a significant implication for the privacy of individuals.

67. Detailed guidance on the content of a PIA is available on the Privacy Commissioner’s website. A PIA can be brief and contained in another document such as a scoping plan. Generally a PIA should address the following privacy principles:

- a. Collecting the information- how will the information be collected?
- b. Storing and keeping it secure- where will it be stored?
- c. Checking the accuracy of the information- how will we assess its accuracy/relevance?
- d. Using or disclosing the information- how will we use/share the information?
- e. Destroying the information- when will we destroy the information?

68. If uncertain on any matters regarding a PIA, employees should consult with the s6(a) and Privacy Officer.



## Roles and Responsibilities

69. All GCSB and NZSIS employees, secondees, s6(a) and contractors are responsible for:

- a. only requesting and accessing personal information that is reasonably required to enable them to carry out their official duties as part of one of GCSB and NZSIS's functions;
- b. ensuring recipients of GCSB and NZSIS personal information are authorised and have measures in place to prevent unauthorised disclosure;
- c. assigning appropriate access controls to information and making good decisions about whether to disclose information;
- d. only assigning a unique identifier when needed; and
- e. seeking advice from a line manager or a Privacy Officer in cases of uncertainty.

70. GCSB and NZSIS Compliance and Policy/Risk Teams are responsible for:

- a. ensuring all operational policy considers privacy and is consistent with the legal obligations set out in this policy; and
- b. investigating breaches together with the Privacy Officers.

71. Staff with management responsibilities are responsible for:

- a. ensuring all GCSB and NZSIS employees, secondees, s6(a) and contractors only request and access personal information that is reasonably required to enable them to carry out their official duties as part of one of GCSB or NZSIS's functions; and
- b. ensuring all privacy breaches are reported in line with this Policy.

72. Privacy Officers are responsible for:

- a. liaising with the Legal team, if required, regarding the interpretation and application of this policy;
- b. providing advice to employees regarding personal information;
- c. encouraging compliance with the Privacy Act and this policy;
- d. advising SLT and the Director-General on the adequacy of GCSB and NZSIS systems for dealing with personal information and compliance with the Privacy Act and steps to be taken to promote robust privacy practices; and

- e. dealing with requests to the agencies under the Privacy Act and working with the Privacy Commissioner to support investigations conducted in relation to GCSB and NZSIS.

73. The Directors-General and SLT are responsible for:

- a. ensuring GCSB and NZSIS have systems and processes in place to promote robust privacy practices, dealing with requests made under the Privacy Act, and governance arrangements for privacy breaches and incident management.

## Previous Policy Revoked

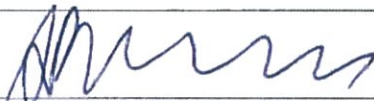


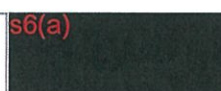
74. This policy revokes and replaces:

- a. JPS – 009 Privacy (approved on: 22 June 2018)




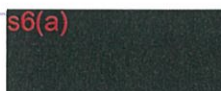
<i>Joint Policy Statement - 009</i>	<i>Page: 18 of 21</i>
<i>JPS - Privacy</i>	<i>Version: 1.0</i>
	<i>Date: 1 December 2020</i>

## Approvals

### GCSB Approval

Approved by:	Director-General, GCSB 
Approval date:	30/11/20
Policy Owner:	Chief Legal Adviser
Current incumbent:	s6(a) 
Policy Administrator:	Compliance and Policy Manager
Current incumbent:	s6(a)  Contact number: s6(a) 

### NZSIS Approval

Approved by:	Director-General, NZSIS 
Approval date:	30/11/20
Policy Owner:	General-Counsel
Current incumbent:	s6(a) 
Policy Administrator:	Compliance and Risk Manager
Current incumbent:	s6(a)  Contact number: s6(a) 

**Effective date: 1 December 2020**

**Review date: 1 December 2023**

## Appendix 1 – Privacy Officers

### NZSIS Privacy Officer

Privacy Officer	General Counsel		
Current incumbent:	s6(a)	Contact number:	s6(a)

### GCSB Privacy Officer

Privacy Officer	Chief Legal Adviser		
Current incumbent:	s6(a)	Contact number:	s6(a)