GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Policy Statement: **PS - 131** File: **A1317608**

Personal Information Policy for Information Collected for Operational Purposes

Purpose

1. The purpose of this policy is to provide GCSB employees with principles for:
    a. assessing the proportionality of collecting personal information;
    b. accessing and using personal information when performing a statutory function or as approved by a suitably senior member of staff;
    c. disclosing personal information only when performing one of GCSB's statutory functions, to the extent required and only when the recipient of that information will protect it as approved by GCSB; and
    d. taking reasonable steps to ensure personal information is up to date, complete, relevant and not misleading.
2. Within this policy, "GCSB employees" refers to anyone employed by or acting on behalf of GCSB.
3. See **annex one** for the text of section 25B from the GCSB Act 2003 and the relevant Information Privacy Principles from the Privacy Act 1993.

Relevant material

4. This policy addresses GCSB's obligations to protect personal information as required under the GCSB Act (in particular, sections 25A and 25B) and the Privacy Act (in particular, sections 6, 27-29, 57 and 81).
5. Further provisions for protecting personal information are contained in the Protective Security Requirements, the Information Security Manual, and New Zealand Signals Intelligence Directive 3 SIGINT Security, as well as related GCSB policy documents, including the Data Retention Policy, and the procedural guidance contained in Responding to Information Requests.
6. Other relevant legislation includes the:
    a. Public Records Act 2005;
    b. Protected Disclosures Act 2000;
    c. Official Information Act 1982; and
    d. New Zealand Security and Intelligence Service Act 1969.

Definitions

7. The Privacy Act 1993 defined "personal information" as any information about an identifiable individual. An identifiable individual is any person regardless of nationality.
8. "Operational purposes" means for the purposes of conducting GCSB's statutory functions; that is, information assurance and cybersecurity, intelligence gathering and analysis, and cooperation with other entities to facilitate their functions.
9. Protected Information, a category of data in information assurance and cybersecurity activities, is personal information. If a warrant or authorisation or agreement with an entity receiving services from GCSB imposes special conditions on protected information outside of what is required by this policy, the higher standard must be followed.

Scope

10. This policy applies to all personal information that GCSB requests, collects, processes, retains, analyses, disseminates, exchanges, and deletes for operational purposes.
11. For information about employee (including contractors, integrees and anyone else acting on behalf of GCSB) personal information, consult *PS 130 Personal Information Policy for Employee Information*.
12. GCSB must ensure that any personal information provided to NZSIS, NZDF or NZ Police to facilitate their functions as part of an approved 8C request for assistance also complies with this policy. If there are any conflicts between this policy and the limitations and restrictions placed on the requesting entity, this will be resolved through the 8C request approval process. Any issues should be directed to the GCSB Legal team.

Audit

13. The Compliance and Policy Manager will consider and assess compliance with all or parts of this policy, at least annually, when conducting audits of operational activity.
14. The Compliance and Policy Manager will consult the Inspector General and the Privacy Commissioner prior to carrying out any audits in relation to this policy. This will ensure the Inspector General and Privacy Commissioner are able to request audits of specific areas.
15. The Director must advise the Privacy Commissioner of the results of audits conducted under this policy. The Privacy Commissioner may provide a report to the Inspector-General of Intelligence and Security if applicable.

Review

16. This policy will be reviewed not more than every three years and, if appropriate, will be reviewed in consultation with the Inspector-General of Intelligence and Security and the Privacy Commissioner.

Privacy Officers

17. The position of Privacy Officer is responsible for encouraging compliance with the Privacy Act. In practice, this means providing advice to staff regarding personal information and privacy matters.

18. The Privacy Officer(s) is an advisory position on privacy matters. If staff members have any queries about privacy issues, they should be directed to the Privacy Officer(s) at privacy@gcsb.govt.nz. The Privacy Officer(s) will be the conduit to any other relevant teams.

Policy

Statutory Framework

19. Section 25B(b) of the GCSB Act 2003 requires GCSB to:
    a. collect personal information only when reasonably necessary for fulfilling a lawful purpose connected with a function of GCSB;
    b. protect personal information;
    c. use information that is accurate; and
    d. retain personal information only for as long as it is needed.

20. In addition, GCSB is required to adhere to the following Information Privacy Principles from the Privacy Act 1993:
    a. Principle 6: Access to personal information;
    b. Principle 7: Correction of personal information; and
    c. Principle 12: Unique identifiers.

GCSB Act 2003 principles to protect personal information

Interpretations

The nature of intelligence-gathering

21. Intelligence is information that results from the collection, collation, and analysis of data to provide the recipient with new information that informs policy-making, decision-making and actions. GCSB specialises in the collection of 'secret' intelligence, i.e. intelligence that is derived from information that the originator does not want to reveal. Crucially, this can often involve targeting of individuals.

22. When intelligence collection agencies target an individual, they do this for two reasons:
    a. they wish to obtain information that the person is believed to possess, information that meets or sheds light on an intelligence requirement, and/or
    b. they wish to obtain information about the person's activities, associates and intentions, because that person or their activities, associates and/or intentions are relevant to an intelligence requirement.

    Particularly in the latter case, the goal of collection and analysis is to understand information such as the intents and motivations of the target as accurately as possible and use that understanding to provide unique insights in relation to the intelligence requirement.

23. Achieving this goal requires collection of (often unknown) information, followed by an assessment or determination of whether that information is useful and, therefore, is intelligence. In short, even after collection, whether a particular piece of information is considered intelligence is often not immediately obvious or knowable. It may require the information in question to be considered in context and/or analysed. At a practical level, this means that the nature of intelligence-gathering:
    a. is often covert; and

b. is often undertaken without full knowledge in advance by the collector of what information will be uncovered; and
c. is such that it can be a narrow lens through which to view or understand a target - the information collected may offer only a partial view of a person or subject, it can be disjointed unless placed alongside other information, and it is not necessarily always accurate; and
d. is such that the value of information *as intelligence* may not be revealed until the information has subsequently been analysed – and/or combined with other information/intelligence.

24. The nature of intelligence-gathering is also intrusive. The act of collection often provides direct access to the views and intentions of individuals in real time. These views and intentions may be private and not ones the target would be prepared to publicly reveal. For that reason, all information collected by GCSB (including personal information) must only be collected, held and used under lawful authority and in accordance with the applicable statutory framework, including the GCSB Act 2003 and the Government's national intelligence priorities

Interests and constraints of national security

25. The 'interests and constraints of national security' refers to the consequences for, and limits imposed by, the overarching goal of protecting of New Zealand, New Zealand interests and New Zealanders against adverse security outcomes.

26. In light of the recently-determined 'all hazards' approach to the meaning of 'national security',[1] such interests and constraints are likely to be numerous and changeable, depending on circumstances. For example, in some cases the interests of national security will indicate perfect accuracy of information is required. In others, the constraints of national security will indicate that accuracy must be foregone to protect tradecraft or a source.

Section 25B(a): Collecting personal information

27. GCSB deliberately or inadvertently collects information about people for a range of purposes, all of which are connected to its functions. Due to the nature of GCSB's statutory roles, the collection of personal information cannot always take place directly from the individual in question, may be derived from any number of open or covert information assets and resources, and is not always undertaken with the consent or even knowledge of the individual in question.

28. GCSB will apply its existing processes in relation to the collection of information when collecting personal information.

29. These processes include only collecting information where:
    a. the collection is covered by a relevant interception warrant, access authorisation, or other lawful authority; and
    b. GCSB assesses that it is reasonably necessary to collect the information in order to perform one of GCSB's statutory functions.

Assessing reasonableness

30. While it will not always be possible to have complete information to inform the assessment of whether collection is reasonably necessary, there must be a reasoned

[1] Refer DES Min (13) 6/1 and the National Security and Resilience Plan.

basis for the assessment that it is. Information that may be considered when making such an assessment may include:

a. knowledge about the nature of the information to be collected;
b. knowledge derived from other available intelligence.

31. There is a reasoned basis to assess that collection is reasonably necessary for the performance of a function where this information will directly or indirectly contribute to the performance of one of those functions

Collection must be proportionate

32. In many respects, personal information can be considered as more sensitive than non-personal information. This means that GCSB must consider the value of the information to be collected, taking into account the sensitivity of that information.

33. Interference with an individual's right to privacy must also be considered against the extent to which interference is justified by the need to perform GCSB's statutory functions.

34. The sensitivity of personal information also varies. This must also be taken into account when collecting personal information.

Section 25B(b): Protecting personal information

Existing protections

35. As an intelligence agency, GCSB collects large amounts of information daily. This occurs under a strict legal and policy framework and, for as long as it holds information, GCSB stringently protects it for national security, operational and reputational reasons.

36. GCSB has the skills and resources to ensure the protection of personal information in a variety of ways. It has implemented measures focusing on such matters as the design and management of secure information storage and transmission facilities; the classification and tracking of information; and mandatory information-handling procedures.

37. These existing protections employed by GCSB in relation to its personal information holdings are adequate for safeguarding against loss, unauthorised access or use, modification, disclosure and misuse.

Access to and use of information

38. Personal information held by GCSB must only be accessed or used by:

a. staff in GCSB who require access for the purpose of performing a statutory function, as approved by a suitably senior member of staff; or
b. staff in other agencies as approved by a suitably senior member of GCSB staff and subject to any conditions imposed by GCSB.

Disclosing personal information

39. GCSB staff must only disclose information, including personal information:

a. in the performance of GCSB's functions;
b. to the extent required; and
c. only when the recipient of that information will protect that information appropriately and use it only as approved by GCSB.

Section 25B(c): Ensuring the accuracy of personal information

40. GCSB must take reasonable steps to ensure that all personal information held is accurate, up to date, complete, relevant and not misleading. However, the technical

means used to collect intelligence, including personal information, results in potentially incomplete information being collected, held and used by GCSB.

41. In circumstances where the potential impact of the use of the intelligence is great, there may be a greater need for GCSB to take additional steps to ensure accuracy.

42. Existing processes record the decisions made and the steps taken. These steps may be captured in formal reports, email or other electronic or physical documents.

Section 25B(d): Retaining personal information

43. GCSB must not keep personal information longer than is required for the purposes for which the information may lawfully be used. For more information on this policy, consult *PS-128 Data Retention and Disposal Policy.*

Information Privacy Principles from the Privacy Act 1993

Principles 6 and 7: Requests for access to and correction of personal information

44. GCSB's processes for dealing with access to and correction of personal information are set out in *PP-1007 Responding to Requests for Information*.

Principle 12: Unique identifiers

45. GCSB has good reason to create and assign unique identifiers in some circumstances in order to enable it to carry out its functions efficiently. This includes identifiers such as cover names. See *PS – 103 Allocation and Control of Cover Names Within the GCSB* for more information.

Use of cover names

46. GCSB may apply unique identifiers to individuals for security purposes. Secure processes support the ongoing performance of GCSB's functions. These unique identifiers may be in the form of cover names. Cover names will usually be applied to an individual who remains unaware of its existence.

Duplication

47. GCSB will consult other relevant agencies to ensure that cover names applied to individuals have not previously been used. GCSB may adopt cover names already applied by another agency if GCSB is a participant in a joint activity.

48. The staff member responsible for assigning the cover name must consult Registry or the relevant team if appropriate.

When to assign cover names

49. Cover names can be assigned at any time as long as it is necessary to enable GCSB to carry out a function efficiently. For example, while working under section 8B of the GCSB Act, it may be efficient to assign a cover name to an individual that would allow for more open discussion of the individual's activities while still protecting their security and right to privacy.

Establish identity before assigning unique identifier

50. If it is necessary to assign a unique identifier to an individual or individuals, all reasonable steps must be taken to ensure that this occurs only in respect of individuals whose identity is clearly established.

51. In the context of GCSB a clearly established identity may not be the same as an individual's true identity. For example, the individual may be only ever known by a pseudonym or may be assigned a temporary identifier until their true identity is established.

Other Considerations

GCSB Policy Procedures

52. Directorates may give effect to the principles in this policy by creating individual policy procedures in line with *PS-100 Joint GCSB and NZSIS Policy Framework*.

Privacy Impact Assessments

53. In instances where a project:
    a. involves personal information;
    b. involves information that may be used to target or identify individuals;
    c. may result in surveillance of individuals, or intrusions into their personal space of bodily privacy; or
    d. may otherwise affect whether people's reasonable expectations of privacy are met;

    then it may be appropriate to conduct a Privacy Impact Assessment (PIA) in accordance with the Privacy Commissioner's guidance (available on their website).

54. These assessments can be used to identify whether a proposed project is likely to impact on the privacy of individuals affected by the project.

55. PIAs are voluntary and do not need to be conducted for each project.

Future reform of legislation

56. Future reform of the Privacy Act may require mandatory reporting of all data breaches to the Privacy Commissioner, as well as giving that office holder the power to issue compliance notices. The results of the 2015 legislative review of the GCSB and NZSIS governing legislation will likely also have implications for this policy.

57. If these changes are enacted, this policy will be updated to reflect the new requirements.

Responsibilities

Director

1. The Director is responsible for the ownership of this policy and overall compliance with this policy.
2. The Director is responsible for advising the Privacy Commissioner of the results of audits conducted under this policy.

Privacy Officer(s)

3. The Privacy Officers are responsible for providing advice to staff regarding personal information.

Compliance and Policy Manager

4. The Compliance and Policy Manager is responsible for auditing compliance with this policy and consulting the Inspector General and Privacy Commissioner prior to carrying out these audits.
5. The Compliance and Policy Manager is also responsible for reviewing this policy not more than every three years. If appropriate, this will be done in consultation with the Inspector General and Privacy Commissioner.

All Managers

6. All managers are responsible for ensuring their employees comply with this policy.

All GCSB employees

7. All GCSB employees are responsible for
    a. assessing the proportionality of collection;
    b. accessing and using personal information only when performing a statutory function or as approved by a suitably senior member of staff;
    c. disclosing personal information only where performing one of GCSB's statutory functions, to the extent required and only when the recipient of that information will protect it as approved by GCSB; and
    d. taking reasonable steps to ensure personal information is up to date, complete, relevant and not misleading.

Annex one

GCSB Act 2003

25B Principles to protect personal information

The principles referred to in section 25A(1) are as follows:

(a) the Bureau must not collect personal information unless—

  (i) the information is collected for a lawful purpose connected with a function of the Bureau; and

  (ii) the collection of the information is reasonably necessary for that purpose, having regard to the nature of intelligence gathering:

(b) the Bureau must ensure—

  (i) that any personal information it holds is protected by such security safeguards as it is reasonable in the circumstances to take against—

    (A) loss; and

    (B) access, use, modification, or disclosure, except with the authority of the Bureau; and

    (C) other misuse; and

  (ii) that if it is necessary for any personal information that it holds to be given to a person in connection with the provision of a service to the Bureau, everything reasonably within the power of the Bureau is done to prevent unauthorised use or unauthorised disclosure of the information:

(c) the Bureau must not use personal information without taking such steps (if any) as are, in the light of the interests and constraints of national security and the nature of intelligence gathering, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading:

(d) the Bureau must not keep personal information longer than is required for the purposes for which the information may be lawfully used.

Section 25B: inserted, on 26 September 2013, by section 26 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Privacy Act 1993 - Information Privacy Principles

Principle 6

Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—

(a) to obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) to have access to that information.

(2) Where, in accordance with subclause (1)(b), an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5.

Principle 7

Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled—

(a) to request correction of the information; and

(b) to request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3), the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1), the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 12

Unique identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any 1 or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of subpart YB of the Income Tax Act 2007.

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

Approval Table

Approved by:

	Director, GCSB	Signed:	
Effective date:	29 July 2016		
Review date:	29 July 2019		
Owner:	Associate Director		
Current incumbent:			
Administration officer:	Policy Analyst		
Current incumbent:		Contact number:	

Revision/modification

Date	Summary of changes	Approved/ Rejected	Approval Authority	File No