GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

New Zealand Security Intelligence Service
Te Pā Whakamarumaru

Joint Policy Statement: JPS - 009

JPS - 009 Privacy

Policy Owner	Director, Strategy and Governance, GCSB Deputy Director-General, NZSIS
Policy Administrator	Compliance and Policy Manager, GCSB Compliance and Risk Manager, NZSIS
Approval Authority	Director-General, GCSB Director-General, NZSIS
Approval Date	22/6/18
Review Date	Three years from signing

Contents

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 1993. 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 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 1993 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:

- Intelligence collection and analysis;
- Protective security, advice and assistance;
- Information assurance and cybersecurity activities (GCSB only);
- Co-operation with other public authorities to facilitate their functions;
- Co-operation with other entities to respond to imminent threat; and
- 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 covert information assets, resources or approaches. 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, 6(a) 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).

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:** non-compliance with any of the legal obligations and principles contained within this policy.
    d) **Torts:** 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 1993

15. The Privacy Act 1993 is the key piece of legislation governing the protection of personal information. The Privacy Act sets out 12 Information Privacy Principles (IPPs) governing personal information. IPPs 2, 3 and 4b do not apply to GCSB and NZSIS. 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(fa), 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 2003 and the Credit Reporting Privacy Code 2004, are:

    a. Telecommunications information cannot be disclosed under IPP 11(fa) where the disclosure may be sought in accordance with a business records direction under the ISA.

    b. When conducting a security clearance assessment, credit information can only be disclosed in accordance with an access agreement. An access agreement is a written agreement between NZSIS and a credit reporter that provides access to credit information for use in security vetting. Credit information may be disclosed to GCSB and NZSIS for the performance of their other functions in accordance with IPP 11(fa).

18. GCSB and NZSIS must be aware of these restrictions when requesting information from telecommunications providers and credit reporters for vetting purposes. Further information on the Privacy Codes can be found on the Privacy Commissioner's website.[1]

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

[1] www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/

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 they 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

23. In New Zealand, the courts recognise two potential torts of invasion of privacy:
    - 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
    - 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).
24. 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, or where they are undertaking highly intrusive surveillance.

Policy

25. 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, reasonableness. In practice, this is considered as part of existing processes, including when developing warrant applications and operational documentation.
26. GCSB and NZSIS must consider privacy when developing new policies and procedures.

Privacy officers

27. Each agency must have at least one privacy officer (section 23 of the Privacy Act). The Privacy Officer(s) is an advisory position on privacy matters. A Privacy Officer is responsible for:
    a) Encouraging compliance by the agency with the privacy principles;

b) Dealing with information requests made to the agency pursuant to the Privacy Act;

c) Working with the Commissioner on investigations conducted pursuant to Part 8 of the Privacy Act in relation to the agency;

d) Otherwise ensuring compliance by the agency with the Privacy Act; and

e) Advising staff on privacy matters relating to the agency.

28. 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)

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.

29. 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.

30. 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.*

31. 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.

32. 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 sources, accesses and other sensitive material from unauthorised access.

33. 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 the access to information. Where technically possible, attempts to inappropriately access information are monitored across both agencies by the Protective Monitoring Centre and agency-specific processes (for example, audits).

34. 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).

35. 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 and IPP 11.

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.

36. 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. 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.

37. 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.

38. 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

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

39. GCSB and NZSIS should take all reasonable steps available to ensure that the information obtained is accurate, up-to-date, complete and relevant before using the information in the performance of any statutory functions.

40. 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.

41. For GCSB, validating the details surrounding the collected information 6(a) 6(a) is the most important aspect of this IP because GCSB is not an assessment agency and hence cannot speak to the intention of the subject.

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.

42. 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.

43. 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.

44. The ISA also enables the 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.

45. In accordance with the specified exemptions, the agencies can disclose personal information where the agencies believe 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.

46. As well as privacy considerations, GCSB and NZSIS also limit the disclosure of information to protect accesses, sources and equities. Limiting for one purpose protects the information for the other purpose as well.

47. GCSB and NZSIS 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.

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 6(a) 6(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 6(a)

IPP 12: unique identifiers

IPP 12 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 12 where it is necessary to carry out their functions efficiently. The use of covernames (known as codenames to NZSIS) is required to protect the identities of the subjects of investigation as well as human sources. For example it may be necessary to assign a covername to an individual to allow for more open discussion of the individual's activities while still protecting their security and privacy.

53. This principle only applies when assigning covernames (and other unique identifiers) to individuals; it does not apply to covernames for operations, projects or other activities conducted by GCSB and NZSIS.

54. GCSB and NZSIS staff should speak to the Privacy Officers if they intend to use unique identifiers for individuals for any other purpose. More detail about GCSB cover names is contained in PS – 103 Allocation and Control of Cover Names within GCSB.

Privacy breach and incident management

55. 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 6(a) and other relevant teams.

56. The Compliance team, in cooperation with the Privacy Officer(s), will:

a) attempt to contain the breach and perform an initial investigation;

b) either notify the impacted individual/s or record the reasons why the individual/s were not notified, after considering any security implications;

c) inform the Inspector-General of Intelligence and Security, if required by the relevant Compliance Framework;

d) consider notifying the Privacy Commissioner. Any reporting to the Privacy Commissioner will require the Director-General's approval, unless it is mandatory under any statute; and

e) report to SLT on the breach, where required in accordance with the relevant Compliance Framework.

57. 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

58. 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.

59. The Privacy Commissioner's guidance (available on their website)[2] 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
    may otherwise affect whether people's reasonable expectations of privacy are met.

60. GCSB and NZSIS should write a PIA where seeking to undertake novel collection methods or doing something exceptional with personal information, for example seeking to create a Direct Access Agreement for accessing personal information from other government departments.

[2] Link to the Privacy Impact Assessment guidance document

61. 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.

62. If uncertain whether a PIA is required, employees should consult with the Knowledge Manager (NZSIS only) and Privacy Officer(s).

Roles and Responsibilities

63. All GCSB and NZSIS employees, secondees 6(a) and contractors are responsible for:
    - 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;
    - ensuring recipients of GCSB and NZSIS personal information are authorised and have measures in place to prevent unauthorised disclosure;
    - Assigning appropriate access controls to information and making good decisions about whether to disclose information;
    - only assigning a unique identifier when needed; and
    - seeking advice from a line manager or a Privacy Officer in cases of uncertainty.

24. GCSB and NZSIS Compliance and Policy/Risk Teams are responsible for:
    - ensuring all operational policy considers privacy and is consistent with the legal obligations set out in this policy
    - investigating breaches together with the Privacy Officers.

64. Staff with management responsibilities are responsible for:
    - ensuring all GCSB and NZSIS employees, secondees, 6(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
    - ensuring all privacy breaches are reported in line with this Policy.

65. Privacy Officers are responsible for:
    - liaising with the Legal team, if required, regarding the interpretation and application of this policy;

- providing advice to employees regarding personal information;
- encouraging compliance with the Privacy Act and this policy;
- 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
- 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;

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

67. This policy revokes and replaces:
    - Privacy Policy (NZSIS); and
    - PS-131 Personal information policy for information collected for operation purposes (GCSB).

Approvals

GCSB Approval

Approved by:	Director-General, GCSB		
Approval date:	21/6/18		
Policy Owner:	Director, Strategy and Governance, GCSB		
Current incumbent:	6(a), 9(2)(a)		
Policy Administrator:	Compliance and Policy Manager		
Current incumbent:	6(a), 18(c)(i)	**Contact number:**	6(a), 18(c)(i)

NZSIS Approval

Approved by:	Director-General, NZSIS	Rebecca Kitteridge	
Approval date:	22/6/18		
Policy Owner:	Deputy Director, NZSIS		
Current incumbent:	6(a), 18(c)(i)		
Policy Administrator:	Compliance and Risk Manager		
Current incumbent:	6(a), 18(c)(i)	**Contact number:**	6(a), 18(c)(i)

Effective date: 29 June 2018 ***Review date: 29 June 2021***

Summary of Minor Amendments

Date	Summary of changes	Approval Authority	Signature

Appendix 1 – Privacy Officers

NZSIS Privacy Officers

Privacy Officer	Chief Legal Advisor		
Current incumbent:	6(a), 18(c)(i)	**Contact number:**	6(a), 18(c)(i)
Privacy Officer	Senior OIA Advisor		
Current incumbent:	6(a), 18(c)(i)	**Contact number:**	6(a), 18(c)(i)

GCSB Privacy Officers

Privacy Officer	Chief Legal Adviser		
Current incumbent:	6(a), 9(2)(a)	**Contact number:**	6(a), 9(2)(a)
Privacy Officer	Principal Adviser, Strategic Performance Policy		
Current incumbent:	6(a), 9(2)(a)	**Contact number:**	6(a), 9(2)(a)

Appendix 2 - Information Privacy Principles that apply to GCSB and NZSIS

Principle 1

Purpose of collection of personal information

Personal information shall not be collected by any agency unless—

a) the information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) the collection of the information is necessary for that purpose.

Principle 4

Manner of collection of personal information

Personal information shall not be collected by an agency—

(a) by unlawful means;

Principle 5

Storage and security of personal information

An agency that holds personal information shall ensure—

(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) loss; and

(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) other misuse; and

(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

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 8

Accuracy, etc, of personal information to be checked before use

(1) An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, 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.

Principle 9

Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10

Limits on use of personal information

(1) An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,—

(a) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or

(b) that the use of the information for that other purpose is authorised by the individual concerned; or

(c) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that the use of the information for that other purpose is necessary to prevent or lessen a serious threat (as defined in section 2(1)) to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(e) that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) that the information—

(i) is used in a form in which the individual concerned is not identified; or

(ii) is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) that the use of the information is in accordance with an authority granted under section 54.

(2) In addition to subclause (1), an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.

Principle 11

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—

(a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

(c) that the disclosure is to the individual concerned; or

(d) that the disclosure is authorised by the individual concerned; or

(e) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious threat (as defined in section 2(1)) to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(fa) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or

(g) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) that the information—

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is in accordance with an authority granted under section 54.

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.