Council Policy

Policy Title:	**Closed Circuit Television (CCTV) Policy 2022**
Responsibility:	Ruapehu District Council Security Manager
First Adopted:	2022
Review Frequency:	Five yearly, or as otherwise required
Last Reviewed:	May 2022
Next Review Due:	May 2027

1 Policy Objectives

1.1 This Policy:

(a) defines the purpose of deploying Ruapehu District Council ("Council") Closed Circuit Television Systems ("CCTV");

(b) ensures that Council's employees and contractors comply with best practice, transparency and accountability principles when operating Council's CCTV cameras; and

(c) ensures Council complies with the requirements of the Privacy Act 2020 (the Act).

2 Definitions

2.1 Authorised Person

Refers to CCTV contractors and Council staff who are authorised to use and access Council's CCTV network and footage. The Information Systems Governance Group ("ISGG") approves authorised contractors and staff who need to access records as part of their role/function.

2.2 Agency

Section 4 of the Act defines 'Agency' to mean a person, business, or organisation that collects and holds personal information about other people. An individual acting in their personal or domestic capacity is not an agency.

2.3 Closed Circuit Television (CCTV)

CCTV is a closed system consisting of video cameras, display devices (monitors) and wired or wireless data networks used to transfer images from fixed videos cameras to monitors. The video surveillance system, in additional to cameras and monitors, often include other devices, such as servers, disk storage and computers that allow storing and processing of video.

2.4 Footage/s

Information collected by the surveillance system may include:

- Video and still footage
- Number plates (from Automatic number plate recognition cameras)
- Metadata including time, date and location
- Summary of event, location, date and time (a catalogue of notable events in recorded footage)

2.5 The Information System Governance Group (ISGG)

The ISGG is made up of the Executive Leadership Team, the Information Technology team and the Manager Information Management, People, Capability and Safety. The ISGG formulates strategies with the guidance of the ICT Strategy and work within this strategy to establish and drive the IT Roadmap for the organisation.

2.6 Mobile Cameras

Refers to cameras that can be moved from one location to another to capture incidents of interest being investigated or researched by Council.

2.7 Personal Information

Section 7 of the Privacy Act 2020 states that Personal Information:

(a) *means information about an identifiable individual and*

(b) includes information relating to a death that is maintained by the Register-General under the Births, Deaths, Marriages, and Relationship Registration Act 1995 or any formers Act (as defined in section 2 of the Births, Deaths, Marriages and Relationship Registration Act 1995).

2.8 Public Spaces

Spaces that are accessible to the public such as streets, footpaths, public parks and public facilities.

2.9 Non-covert cameras also known as 'public facing' cameras

Refers to CCTV cameras that are visible and people are made aware that they are being monitored. For instance, signs are erected informing people that CCTV cameras are operating within the vicinity they are in. Part 3, Section 22 (Information privacy principle 3 (1)) of the Privacy Act 2020 enforces agencies to disclose when they are collecting people's information.

2.10 Covert cameras

Refers to hidden CCTV or mobile cameras. Part 3, Section 22 (Information privacy principles (3) and (4)) of the Privacy Act 2020 gives agencies the power to collect information from subjects without informing them, if they believe, on reasonable grounds, that telling them about the collection will harm the individual concerned, or it would undermine the purpose of the collection of information. (See Schedule 1).

2.11 Production Order

Production Orders are orders applied for under section 71 of the Search and Surveillance Act 2012, requiring a person or organisation (such as a business) to produce documents to enforcement agencies as evidential material of a specified offence.

Production Orders are issued pursuant to section 74 of the Search and Surveillance Act 2012 by issuing officers, i.e., a Judge or a person authorised to act as an issuing officer. When issuing a Production Order, Section 72 of the Search and Surveillance Act 2012 must be satisfied.

Section 72 states:

The conditions for making a production order are that there are reasonable grounds:

(a) to suspect that an offence has been committed, or is being committed, or will be committed (being an offence in respect of which this Act or any enactment specified in column 2 of the Schedule authorises an enforcement officer to apply for a search warrant); and

(b) to believe that the documents sought by the proposed order:
  (i) constitute evidential material in respect of the offence; and
  (ii) are in the possession or under the control of the person against whom the order is sought, or will come into his or her possession or under his or her control while the order is in force.

2.12 Search Warrant

The Search and Surveillance Act 2012, requires the New Zealand Police ("Police") to apply to the courts for a search warrant if they want to search a building or other place, like a vehicle, aircraft or freight container, for evidence that a criminal offence punishable by a jail term has been committed. In Section 103 of the Search and Surveillance Act 2012, the Police must provide a judge or other court official with information to support their belief that evidence is present there. If the judge is satisfied that there are reasonable grounds for the belief, he or she will issue a search warrant.

3 Principles

3.1 This policy supports the following Council focus and community wellbeing outcomes:

(a) Social - safe and healthy communities
- Excellence standards of safety and welfare are promoted and respected.

(b) Environmental - sustaining beautiful environments
- Our environment is accessible, clean, and safe and our water, soil and air meets required standards.

(c) Strong leadership and advocacy
- Council is proactive, transparent, and accountable.

3.2 When deploying and operating CCTV, Council must adhere to the 13 Information Privacy Principles (IPP's) in the Act (see Schedule 1).
These principles deal with issues such as:
(a) being clear about why Council is collecting information about people;
(b) ensuring people know about the cameras and their purpose;
(c) informing the community about how CCTV footages are used;
(d) how Council disclose CCTV footage to others (such as the Police);
(e) how long footage is kept for;
(f) keeping footage safe, and making sure that only authorised people can see the footage; and
(g) rights of access to the information by the individual concerned.

4 Background

4.1 Part 3, Section 22, Information Privacy Principle 1 of the Privacy Act states that:
(1) Personal information shall not be collected 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.

4.2 Section 10 of the Local Government Act 2002, states that:
(1) The purpose of local government is:
(a) to enable democratic local decision-making and action by, and on behalf of, communities; and
(b) to promote the social, economic, environmental, and cultural well-being of communities in the present and for the future.

4.3 To fulfil its purpose, one of Councils key responsibilities is ensuring compliance with a range of laws and regulations that are designed to achieve beneficial community and environmental outcomes. The purpose of Councils CCTV Policy is listed in paragraph 5.1 below. This

purpose aligns with the purpose of local government outlined in paragraph 4.2 above, which encompasses Council's regulatory role.

5 Policy Statement

5.1 PURPOSE

Council's CCTV is installed and operated for one or more of the following purposes:

(a) To facilitate staff and public safety.
(b) To improve security and deter criminal activity in public places (including Council premises and recreational facilities).
(c) To manage traffic movements in particular areas.
(d) To monitor trespass on Council facilities.
(e) To monitor compliance with Council bylaws.
(f) To capture information that is evidence of crime, a health and safety incident and/or staff incidents.
(g) To provide a deterrent to criminal activity.
(h) To enable Police to acquire evidence of criminal behaviour.

5.2 Council's CCTV shall not be deployed in private areas within public spaces and facilities where there is a greater than usual expectation of privacy (e.g., changing rooms, public toilets).

5.3 Council's CCTV shall not be directed at private property except when unavoidable and only to the extent necessary to meet the purposes of the camera deployment.

5.4 DEPLOYING CCTV IN PUBLIC SPACES

Pre-deployment - Council is responsible for deploying CCTV within Council's property, public spaces, and commercial business districts that it oversees. As the CCTV will collect personal information about people and their activities in public places and work environments, careful planning must be undertaken to:

(a) understand the nature of information that will likely be collected;
(b) understand the problems that are to be addressed in a particular area by using CCTV;
(c) ensure that personal information is not collected in an unlawful, unfair, or unreasonably intrusive way;
(d) ensure that personal information is only retained as long as required for the purpose of the CCTV deployment;
(e) ensure that CCTV is deployed in places where it will have a positive impact in deterring crime or assisting in the detection and prosecution of offenders.

5.4.1 **Engagement –** Before deploying crime prevention or public safety CCTV in public places Council will engage with Police to ascertain the most appropriate places to deploy CCTV and to understand the nature of the issues that will be benefit from camera oversight.

5.4.2 Council shall engage with the public to understand concerns and attitudes towards the deployment of crime prevention or public safety CCTV. Engagement must include:
(a) the potential location of camera placements;
(b) the privacy of individuals going about unsuspicious and lawful activity;
(c) the manner in which the cameras will operate (e.g., with or without audio capability; fixed or with panning capability; constant filming or action sensor film).

5.4.3 Where covert CCTV is deployed within Council premises, Council will engage with relevant staff to understand concerns they may have and to advise them of the matters set out in paragraph 5.4.2 above).

5.4.4 **Approval Process -** The establishment, replacement and relocation of all Council CCTV cameras must be approved by the ISGG in conjunction with relevant officers and Community Boards.

5.5 APPROVED CCTV FEATURES

Approved CCTV features may include:

(a) sensor cameras that detect movement within a defined area;
(b) live feed cameras that record footage over a defined period, or continuously over a 24 hour period;
(c) audio capability.

5.6 CCTV REVIEW

A review of Council's CCTV network will be undertaken annually to determine if the deployments continue to meet the purposes sets out in paragraph 5.1 above. If the camera is deemed unnecessary, it will be decommissioned by the end of that financial year.

5.7 TRANSPARENCY

5.7.1 Signage

(a) The site or area that is subjected to camera oversight must include signage indicating to members of the public or staff, of:
    (i) The presence and operation of CCTV in the area; and
    (ii) A point of contact for enquiry about the cameras.
(b) Signage must be readily visible to people using or accessing the location.
(c) Council's website shall include information that details the extent and purpose of Council's CCTV deployments, including a district map broadly indicating the streets or areas where Council has deployed non-covert cameras.
(d) The website advice shall include details about the potential use and disclosure of the footage acquired along with contact details for further enquiry.
(e) This public advice shall be reviewed annually to ensure it is up to date and accurate.

5.8 COVERT CAMERAS

5.8.1 Covert cameras come in the form of mobile cameras. They may only be used for Council's internal purposes in exception circumstance and with the prior approval of the ISGG. Exceptional circumstances may include where there is a strong suspicion of criminal activity or misconduct which breaches Council bylaws or may give rise to health and safety risk to any person or damage to the environment, and which cannot be detected by other means.

5.9 MANAGEMENT OF FOOTAGE

5.9.1 CCTV footage and other information incidental to footage shall be retained on secure servers approved by the ISGG.

5.9.2 Access to the secure servers must be approved by Council's Security Manager. Where Council's Security Manager is unable to perform this responsibility, the power is transferred to the ISGG.

5.10 USE AND DISCLOSURE OF CCTV FOOTAGE

5.10.1 Access by Council Staff and Contractors

5.10.1.2 Access by Council staff and contractors to CCTV information must be authorised by the ISGG. Only trained and authorised persons will be permitted to access Council's stored CCTV footage.

5.10.1.1 Access to and use of CCTV footage by Council staff and contractors shall only be for approved work-related purposes relevant to the purpose for which the camera is deployed.

5.10.1.3 Staff access to CCTV footage may either be granted from time to time or to specific role-based staff for the purposes referred to in paragraph 5.1 above.

5.10.1.4 The Council Security Manager will be responsible for ensuring that all staff access to CCTV information is lawful and necessary. In the case of the Council Security Manager being unable to perform this responsibility, the power is transferred to the ISGG.

5.10.1.5 Inappropriate access to CCTV information may be a breach of Council's Code of Conduct. Investigations into inappropriate access to CCTV information must be approved and managed by the ISGG. In the case of a member of the ISGG being subject to an investigation, the investigation will be managed by a third party.

5.10.2 Access by Police

5.10.2.1 One of the purposes of Council's CCTV is to enable Police to acquire evidence of criminal behaviour. Access to Council's CCTV footage whether live or post an event, shall be subject to a Memorandum of Understanding ("MOU") between Police and Council.

5.10.2.2 Police access to live feed shall be on a 'read only access', which means users are only permitted to view the footage and not make changes to it.

5.10.2.3 Police access to post event CCTV footage is permitted only by either a non-statutory Request for Service ("RFS"), a Production Order or Search Warrant.

5.10.2.4 A RFS from Police must be in writing and must include:

(a) A description with sufficient details to identify the date and time period of the footage required.
(b) An investigation file number or an event number of a matter reported to Police.
(c) The reasons why the information is required. These reasons need to be sufficient to enable Council staff to exercise the discretion to release personal information under the provisions of Section 22 of the Privacy Act 2020. The usual justification for releasing information to Police will arise where sufficient detail is provided to demonstrate that the personal information is required:
    (i) To avoid a prejudice to an investigation, detection, prosecution or prevention of offences;
    (ii) For the conduct of proceedings;
    (iii) To prevent or lessen a serious threat to public health or public safety or the life or health of a person.
(d) Details of the police officer requiring the information.
(e) Approval of the RFS by a police manager.
(f) Except in response to a production order or search warrant, Council's disclosure of CCTV information is not mandatory and is entirely at the discretion of Council.
(g) When disclosing CCTV information, care must be taken to release only the information necessary and proportionate to the request or statutory process.

5.10.3 Access by others

5.10.3.1 Requests for CCTV information made by individuals who require information about themselves shall be managed under the provisions of Section 22 of the Privacy Act 2020, and in particular, Information Privacy Principle 6 (*Access Requests for Personal Information*) and/or Information Privacy Principle 7 (*Correction of Personal Information*) and the provisions of Part 4 of the Privacy Act 2020 (See Schedule 1).

5.10.3.3 All other requests shall be managed under the Local Government Official Information and Meetings Act 1987.

5.11 RETENTION

5.11.1 Unless otherwise required to fulfil the purposes set out in paragraph 5.1 above:

i. CCTV information collected on camera systems monitoring Council premises shall only be retained for 3 months;
ii. CCTV information collected on public spaces cameras such as parks, main streets, etc. is retained for 30 days, after which the footage will be overwritten.

5.11.2 The disposal of CCTV information that is retained beyond the periods stated in 5.11.1 must comply with Public Records Act 2005 and the Archives New Zealand Information and Records Management Standard 2016.

6 Relevant Legislation / Documentation

6.1 The following legislation is relevant to the creation of this policy:

(a) Privacy Act 2020 – in particular Part 3, Information Privacy Principles and Code of Practice 1-13, set out in Section 22 of the Privacy Act 2020;
(b) Local Government Act 2002 - in particular, Section 3 (Purpose) and Section 14 (Principles relating to Local Authorities);
(c) Local Government Official Information and Meetings Act 1987 (LGOIMA);
(d) Search and Surveillance Act 2012 - in particular, Part 2 (Police powers) and Section 74 (Issuing officer may make production order).

6.2 The following documentation is relevant to the creation of this policy:

(a) Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations (Privacy Commission, 2009).
(b) Policy on Crime Prevention Cameras (CCTV) in Public Places (New Zealand Police, 2003).

7 Policy Version Control

Policy drafted by	Policy team Manager Information Technology, People, Capability and Safety in partnership with Simply Privacy Limited
Policy reviewed by	Manager Policy & Strategy Executive Manager Finance & Strategy
Policy reviewed and recommended by the Information System Governance Group (ISGG)	Yes
Policy reviewed and recommended by the Audit and Risk Committee	Yes
Policy reviewed and adopted by Council	Adopted by Council on 25 May 2022

Part 3
Information privacy principles and codes of practice

Subpart 1—Information privacy principles

22 Information privacy principles

The information privacy principles are as follows:

Information privacy principle 1

Purpose of collection of personal information

(1) Personal information must not be collected by an agency unless—

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

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

(2) If the lawful purpose for which personal information about an individual is collected does not require the collection of an individual's identifying information, the agency may not require the individual's identifying information.

Information privacy principle 2

Source of personal information

(1) If an agency collects personal information, the information must be collected from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—

(a) that non-compliance would not prejudice the interests of the individual concerned; or

(b) that compliance would prejudice the purposes of the collection; or

(c) that the individual concerned authorises collection of the information from someone else; or

(d) that the information is publicly available information; or

(e) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention,

detection, investigation, prosecution, and punishment of offences; or

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

(iii) for the protection of 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

(v) to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual; or

(f) that compliance is not reasonably practicable in the circumstances of the particular case; or

(g) that the information—

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

(ii) will 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.

Information privacy principle 3

Collection of information from subject

(1) If an agency collects personal information from the individual concerned, the agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of—

(a) the fact that the information is being collected; and

(b) the purpose for which the information is being collected; and

(c) the intended recipients of the information; and

(d) the name and address of—

(i) the agency that is collecting the information; and

(ii) the agency that will hold the information; and

(e) if the collection of the information is authorised or required by or under law,—

(i) the particular law by or under which the collection of the information is authorised or required; and

(ii) whether the supply of the information by that individual is voluntary or mandatory; and

(f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) the rights of access to, and correction of, information provided by the IPPs.

(2) The steps referred to in subclause (1) must be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if the agency has taken those steps on a recent previous occasion in relation to the collection, from that individual, of the same information or information of the same kind.

(4) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—

(a) that non-compliance would not prejudice the interests of the individual concerned; or

(b) that non-compliance is necessary—

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

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

(iii) for the protection of 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

(c) that compliance would prejudice the purposes of the collection; or

(d) that compliance is not reasonably practicable in the circumstances of the particular case; or

(e) that the information—

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

(ii) will 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.

Information privacy principle 4

Manner of collection of personal information

An agency may collect personal information only—

(a) by a lawful means; and

(b) by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons),—

(i) is fair; and

(ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Information privacy principle 5

Storage and security of personal information

An agency that holds personal information must ensure—

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

(i) loss; and

(ii) access, use, modification, or disclosure that is not authorised by the agency; 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.

Information privacy principle 6

Access to personal information

(1) An individual is entitled to receive from an agency upon request—

(a) confirmation of whether the agency holds any personal information about them; and

(b) access to their personal information.

(2) If an individual concerned is given access to personal information, the individual must be advised that, under IPP 7, the individual may request the correction of that information.

(3) This IPP is subject to the provisions of Part 4.

Information privacy principle 7

Correction of personal information

(1) An individual whose personal information is held by an agency is entitled to request the agency to correct the information.

(2) An agency that holds personal information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances 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) When requesting the correction of personal information, or at any later time, an individual is entitled to—

(a) provide the agency with a statement of the correction sought to the information (a **statement of correction**); and

(b) request the agency to attach the statement of correction to the information if the agency does not make the correction sought.

(4) If an agency that holds personal information is not willing to correct the information as requested and has been provided with a statement of correction, the agency must take such steps (if any) that are reasonable in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensures that it will always be read with the information.

(5) If an agency corrects personal information or attaches a statement of correction to personal information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information.

(6) Subclauses (1) to (4) are subject to the provisions of Part 4.

Information privacy principle 8

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

An agency that holds personal information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

Information privacy principle 9

Agency not to keep personal information for longer than necessary

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

Information privacy principle 10

Limits on use of personal information

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

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

(b) 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

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

(d) 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

(e) that the use of the information for that other purpose is necessary—

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

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

(iii) for the protection of 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 use of the information for that other purpose is necessary to prevent or lessen a serious threat to—

(i) public health or public safety; or

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

(2) In addition to the uses authorised by 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.

Information privacy principle 11

Limits on disclosure of personal information

(1) An agency that holds personal information must not disclose the information to any other agency or to any person 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 disclosure is to the individual concerned; or

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

(d) 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

(e) that the disclosure of the information is necessary—

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

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

(iii) for the protection of 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 to—

(i) public health or public safety; or

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

(g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; 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 necessary to facilitate the sale or other disposition of a business as a going concern.

(2) This IPP is subject to IPP 12.

Information privacy principle 12

Disclosure of personal information outside New Zealand

(1) An agency (**A**) may disclose personal information to a foreign person or entity (**B**) in reliance on IPP 11(1)(a), (c), (e), (f), (h), or (i) only if—

(a) the individual concerned authorises the disclosure to B after being expressly informed by A that B may not be required to

protect the information in a way that, overall, provides comparable safeguards to those in this Act; or

(b) B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to this Act; or

(c) A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in this Act; or

(d) A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or

(e) A believes on reasonable grounds that B is subject to privacy laws of a prescribed country; or

(f) A otherwise believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in this Act (for example, pursuant to an agreement entered into between A and B).

(2) However, subclause (1) does not apply if the personal information is to be disclosed to B in reliance on IPP 11(1)(e) or (f) and it is not reasonably practicable in the circumstances for A to comply with the requirements of subclause (1).

(3) In this IPP,—

prescribed binding scheme means a binding scheme specified in regulations made under section 213

prescribed country means a country specified in regulations made under section 214.

Information privacy principle 13

Unique identifiers

(1) An agency (**A**) may assign a unique identifier to an individual for use in its operations only if that identifier is necessary to enable A to carry out 1 or more of its functions efficiently.

(2) A may not assign to an individual a unique identifier that, to A's knowledge, is the same unique identifier as has been assigned to that individual by another agency (**B**), unless—

(a) A and B are associated persons within the meaning of subpart YB of the Income Tax Act 2007; or

(b) the unique identifier is to be used by A for statistical or research purposes and no other purpose.

(3) To avoid doubt, A does not assign a unique identifier to an individual under subclause (1) by simply recording a unique identifier assigned to

the individual by B for the sole purpose of communicating with B about the individual.

(4) A must take any steps that are, in the circumstances, reasonable to ensure that—

(a) a unique identifier is assigned only to an individual whose identity is clearly established; and

(b) the risk of misuse of a unique identifier by any person is minimised (for example, by showing truncated account numbers on receipts or in correspondence).

(5) An agency may 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 is for a purpose that is directly related to one of those purposes.

Compare: 1993 No 28 s 6