Confidentiality and Information Sharing Policy

November 2018

Contents

1. Netsafe Confidentiality and Information Sharing Policy

PURPOSE

Netsafe Confidentiality and Information Sharing Policy ('Policy') provides guidelines for employees working for Netsafe Incorporated ("Netsafe").

The purpose of the Policy is to ensure that any personal information relating to employees and members of the public who interact with Netsafe services, which is private and not public knowledge or information that an individual has not consented to and/or would not expect to be shared ('Confidential Information'), is adequately secured, protected and only used in appropriate circumstances.

SCOPE

This Policy applies to all employees and advisors engaged by Netsafe.

The Policy is intended to provide a useful framework for ensuring that Confidential Information is appropriately managed and controlled by all Netsafe employees. It should be read in conjunction with Netsafe's Public Sector Information Sharing Guide and with Netsafe's Policies on Privacy, Security, Media and Child Protection.

OBJECTIVES

Applying this Policy will ensure that:

- Employees understand their obligations and responsibilities relating to the proper acquisition, management and disclosure of Confidential Information;

- Members of the public that interact with Netsafe services are aware of their rights in respect of the acquisition, management and disclosure of their Confidential Information; and

- There is alignment with the relevant legislation (for example, the Privacy Act, Official Information Act, Human Rights Act, Crimes Act, Child Youth and Families Act and Vulnerable Children's Act)

DEFINITIONS

Advisor means any individual or organisation that is engaged (remunerated or voluntary) to provide advisory or consultancy services to Netsafe or any individual working for these organisations in a capacity that has potential to affect employees ability to ensure the safety of members of the public who interact with Netsafe services.

Confidential information means any information that is private and not publicly available or information that an individual has not consented to and/or would not expect to be shared. It Includes person-identifiable information (refer definition below). This information can take many forms including complaint records, employee records, confidential Netsafe organisational information.

Information Owner means the person (in this context usually a party or employee) who is the subject of the information or to whom the information refers.

Informed Consent means the process whereby someone who has the capacity to consent, having been given all the relevant information, arrives at a decision as to whether or not to agree to the proposed action or actions.

Party means any member of the public who interacts with Netsafe services.

Person-identifiable information ('PII) is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, IRD or ACC or passport number etc. It is information where the person can be recognised by persons other than themselves.[1]

PRINCIPLES

Confidential information about employees and parties should always be:

- Obtained fairly and with Informed Consent as appropriate;
- Acquired only for the purposes of providing Netsafe services, including meeting any legal or statutory obligations relating to those services;
- Maintained as accurate and up-to-date;
- Used only for the purpose for which it was acquired and in accordance with this Policy and the law;
- Retained only as necessary to meet Netsafe, legal or statutory requirements;
- Available to the information owner being the person (employee or party) who is the subject of the information or to whom the information refers to the extent provided for under Principle 6 of the Privacy Act 1993;
- Not disclosed to third parties (including other statutory agencies) without consent other than when disclosure is permitted by the law and then only on a need-to-know basis and 'in confidence'; and
- Protected against loss, improper or unlawful disclosure when it is received, stored, transmitted or disposed of.

[1] There is no hard and fast test for recognition. In some cases, you can argue that a person must be identifiable *beyond* their intimate friends or family. However, in cases that involve sensitive personal information, a person may be considered identifiable if they can be recognised by intimate friends or family only.

CORE ELEMENTS

The Policy has five core elements that together reflect Netsafe's commitment to assuring the confidentiality of information about employees and parties.

1. Commitment to Confidentiality

Netsafe must ensure that the terms of engagement of employees and advisors include a commitment to the protection of Confidential Information and provide that any breaches of that commitment may be regarded as serious misconduct and may result in disciplinary action that could include termination of their engagement.

Employees will treat all information provided by parties, including any communications, as Confidential Information unless the information is publicly available or the party gives Informed Consent for the disclosure of some or all of such information.

2. Provision of Informed Consent

Employees must inform the parties about this Policy and in particular the nature and extent of confidentiality offered in relation to their interaction with Netsafe services.

Employees should assure parties that Confidential Information about them will not be collected, recorded or disclosed to any third party without their Informed Consent except when:

- There is serious danger in the immediate or foreseeable future to the party or others (including the protection of children or young people);
- Disclosure is necessary to comply with the law; or
- In the opinion of the employee, the party's capacity to give Informed Consent is impaired provided that any decision made by the employee to disclose the information is in the best interests of the party and intended, as far as practicable, to safeguard their rights.

Employees will respect the rights of children and young people to receive age appropriate information and have the ability to consent on their own behalf, commensurate with their capacity to do so.

Employees should keep appropriate records to evidence the provision of Informed Consent by a party.

3. Sharing Confidential Information

Netsafe recognises that all staff must act within the legal requirements of the Privacy Act, Children, Young Person's and their Families Act, and other statutes. There are provisions within each of these acts for sharing or requesting access to Confidential Information. In general staff will not share or disclose Confidential Information if they believe that by doing so this will endanger the affected individual.

Netsafe is responsible for:

- Protecting all the Confidential Information they hold, whether in electronic or physical form, and ensuring that they can justify any decision to share that information;
- Always taking into account the interests of the Information Owner whenever Confidential Information is shared with any third party;
- Ensuring that Confidential Information is only shared with the appropriate people in appropriate circumstances;
- Limiting the information shared to the minimum required to reasonably fulfil the purpose of the information sharing and/or meet legal or statutory obligations[2]; and

[2] Relevant legislation includes the Privacy Act 1993, and the Official information Act 1982

- Providing appropriate safeguards for securing the electronic or physical storage and/or transmission of Confidential Information via emails, mail, courier etc.

Staff may be asked to provide Confidential Information to individuals or agencies, for example, Oranga Tamariki, New Zealand Police, Court and Lawyers.

When an individual or agency contacts a staff member for Confidential Information that staff member must first refer to their Manager or Director for clearance before providing the information.

Confidential Information will be only be given after the staff member has identified the person making the request.

All staff will follow Netsafe's guidelines which provide guidance on deciding whether to disclose information either in response to a request for official information or personal information (reactive disclosure), or in the absence of a request (proactive disclosure).

If Netsafe or an employee are required (by warrant or subpoena) to give evidence in Court, confidentiality and the privilege of a party's information should be assumed (in accordance with the party's wishes) until all legal avenues have been explored.

Where employees are uncertain about their obligations and/or responsibilities relating to information sharing and/or disclosure requests they should refer to their Manager, Director and/or the Privacy Officer as appropriate.

4. Abuse of confidentiality

When dealing with Confidential Information of any nature, employees or advisors must be aware of their responsibilities and obligations as provided in this Policy and the law.

It is strictly forbidden for employees or advisors to knowingly browse, search for, or look at any Confidential Information without a legitimate purpose. Actions of this kind will be viewed as a serious breach of this Policy.

5. Assuring Security

Confidential Information held in physical form should be secured in lockable cabinets that are only accessible to employees or advisors that have a genuine need for the information to enable the provision of effective support services to parties.

Wherever possible, Confidential Information that is stored electronically, should be held in secure (preferably 'cloud-based') environments and accessed via secure (password controlled) user- interfaces.

Passwords that permit access to Confidential Information must be kept secure and must not be disclosed to unauthorised persons. Employees or advisors must not use someone else's password to gain access to such information. Actions of this kind will be viewed as a serious breach of this Policy.

Whenever employees and advisors need to carry Confidential Information whilst travelling to, or working from, work-locations they must ensure the security of that information.

Where Confidential Information is stored in electronic form on personal (mobile) electronic devices (e.g. laptops, tablets, USB sticks etc.), such information:

- Must be password secured and only stored on devices that are appropriately secured by their owners;
- Should not be stored on personal devices (e.g. home computers) that are accessible by other people; and
- Should only be stored on personal devices when necessary to provide Netsafe services and limited, as far as practicable to the minimum information required to perform the service.