

## CONFIDENTIALITY POLICY

---

### PURPOSE

The Male Survivors Tairāwhiti ('MST') Confidentiality Policy ('Policy') provides guidelines for all MST trustees, employees, contractors, consultants, advisors and volunteers ('MST people').

The purpose of the Policy is to ensure that any personal information relating to MST people and the male survivors they support, 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 the best interests of the information owner – the person who is the subject of the information or to whom the information refers.

### SCOPE

This Policy applies to all MST people.

The Policy is intended to provide a useful framework for ensuring that Confidential Information is appropriately managed and controlled by all MST people.

### OBJECTIVES

Applying this Policy will ensure that:

- MST people understand their obligations and responsibilities relating to the proper acquisition, management and disclosure of Confidential Information;
- Male survivors 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 (Human Rights Act, Crimes Act, Health and Disability 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 MST or any individual working for MST in a capacity that has potential to affect peer-workers ability to ensure the safety of children and young people.

**Confidential information**

Means any information that is private and not public knowledge 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 male survivor peer-support records, peer-worker records, confidential MST organisational information.

<b>Information Owner</b>	The person (in this context usually MST people or male survivors) who are the subject of the information or to whom the information refers.
<b>Male survivor</b>	Means a male who has experienced sexual, physical, mental, emotional or domestic violence, harm or abuse.
<b>MSA</b>	Is the national organisation Male Survivors, Aotearoa New Zealand, which provides national advocacy for male survivors and governance, coordination and representation for MMO's.
<b>MST people</b>	Means trustees, employees, contractors, consultant, advisors and volunteers who work with or for MST.
<b>Peer-worker</b>	Means an individual engaged as employee or volunteer by MST to provide peer-support services to male survivors.
<b>Personal identifiable information</b>	(‘PII’) Person-identifiable information 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.
<b>Trustee</b>	Means a trustee of MST

## PRINCIPLES

Confidential information about MST people and the male survivors they support, trustees and advisors should always be:

- Obtained fairly and with informed consent as appropriate;
- Acquired only for the purposes of providing MST 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 MST service, legal or statutory requirements;
- Available to the information owner being the person (typically MST people or male survivors) who is the subject of the information or to whom the information refers;
- Not disclosed to third parties without consent other than when disclosure is required 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.

## CORE ELEMENTS

The Policy has six core elements’ that together reflect MST’s commitment to assuring the confidentiality of information about MST people and male survivors.

## 1. Commitment to Confidentiality

MST must ensure that the terms of engagement of MST people 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.

MST people will treat all information provided by male survivors, including any communications, as Confidential Information unless the male survivor gives informed consent for the disclosure of some or all of such information.

## 2. Provision of informed Consent

MST people must inform the male survivors about the relevant provisions of this policy and in particular the nature and extent of confidentiality offered in relation to their engagement with MST services.

MST people should assure male survivors 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 male survivor or others (including the protection of children or young people); or
- Disclosure is necessary to comply with the law (including matter of serious illegality); or
- Disclosure is made under the provisions of a MST approved supervision contract provided that contract has provisions that support the confidentially obligations of peer-workers covered by this Policy; or
- In the opinion of MST people, the male survivor's capacity to give informed consent is impaired provided that any decision made by the peer-worker to disclose the information is in the best interests of the male survivor and intended, as far as practicable, to safeguard his rights.

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

MST people must inform male survivors that they are entitled to withdraw their consent to the collection, recording or disclosure of their Confidential Information at any time except where the maintenance and/or disclosure of such information is required to comply with legal requirements.

## 3. Sharing Confidential Information

MST 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 prioritising the best 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, including with informed consent as appropriate, and in accordance with this Policy, MST's Child Protection Policy or the law;
- Limiting the information shared to the minimum required to reasonably fulfil the purpose of the information sharing and/or meet legal or statutory obligations; and
- Providing appropriate safeguards for securing the electronic or physical storage and/or transmission of Confidential Information via emails, faxes, mail, courier etc.

If MST people are required (by warrant or subpoena) to give evidence in Court, confidentiality and the 'privilege of client information' should be assumed (in accordance with the male survivor's wishes) until all legal avenues have been explored.

Where MST people are uncertain about their obligations and/or responsibilities relating to information sharing and/or disclosure requests they should refer to their Manager and/or the MST Privacy Officer<sup>1</sup> as appropriate.

#### **4. Abusing Privilege**

When dealing with Confidential Information of any nature, MST people must be aware of their responsibilities and obligations as provided in the MST Code of Ethics, this Policy and the law.

It is strictly forbidden for MST people 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**

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.

MST people 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 MST people 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

---

<sup>1</sup> The Privacy Officer for MST is the Manager

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 MST services and limited, as far as practicable to the minimum information required to perform the service.

## **6. Assuring Confidentiality**

Good practice requires that all organisations that handle Confidential Information implement appropriate protocols and procedures to assure the security and proper use of such information.

Given the potential risks for MST relating to the loss or improper disclosure of Confidential Information, MSA reserve the right to audit MMO compliance with this policy including the effectiveness of their protocols and procedures for assuring the security and proper use of Confidential Information.

Any such audits will be conducted under the supervision of the MSA Privacy Officer.