

CONFIDENTIALITY POLICY

PURPOSE

The Male Survivors Aotearoa ('MSA') Confidentiality Policy ('Policy') provides guidelines for peer-workers (both employees and volunteers), trustees and advisors working for the national organisation or MSA Member Organisations ('MMO's).

The purpose of the Policy is to ensure that any personal information relating to peer-workers and the male survivors they support or MSA trustees or advisors, 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 peer worker, male survivor, trustee or advisor who is the subject of the information or to whom the information refers.

SCOPE

This Policy applies to all peer-workers (employees and volunteers), trustees and advisors engaged by MSA or an MMO.

The Policy is intended to provide a useful framework for ensuring that Confidential Information is appropriately managed and controlled by all MSA or MMO peer-workers, trustees and advisors.

OBJECTIVES

Applying this Policy will ensure that:

- Peer-workers, trustees and advisors 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 MSA, and MMO or any individual working for these organisations 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 MSA or MMO organisational information.

Information Owner	The person (in this context usually peer-worker, male survivor, trustee or advisor) who is the subject of the information or to whom the information refers.
Male survivor	Means a male who has experienced sexual abuse and who is supported by a peer-worker required to comply with this Policy.
MMO	Is an organisation that is affiliated via formal membership agreement as an official Member Organisation of MSA.
MSA	Is the national organisation Male Survivors, Aotearoa New Zealand, which provides national advocacy for male survivors and governance, coordination and representation for MMO's.
Peer-worker	Means an individual engaged as employee or volunteer by MSA or an MMO to provide peer-support services to male survivors of sexual abuse.
Personal identifiable information	('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.
Trustee	Means a trustee of MSA or an MMO

PRINCIPLES

Confidential information about peer-workers 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 MSA or MMO 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 MSA or MMO service, legal or statutory requirements;
- Available to the information owner being the person (peer-worker, male survivor, trustee or advisor) 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 seven core elements' that together reflect MSA's commitment to assuring the confidentiality of information about peer-workers, male survivor's and MSA and MMO trustees and advisors.

1. Commitment to Confidentiality

MSA and MMO's must ensure that the terms of engagement of peer-workers (employees and volunteers), trustees 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.

Peer-workers 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

Peer-workers 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 MSA or MMO services.

Peer-workers 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 MSA and MMO 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 the peer-worker, 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.

Peer-workers 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.

Peer-workers 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

MSA and MMO's are 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, MSA'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 MSA, and/or MMO or a peer-worker 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 peer-workers 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 MSA Privacy Officer¹ as appropriate.

4. Abusing Privilege

When dealing with Confidential Information of any nature, peer-workers, trustees or advisors must be aware of their responsibilities and obligations as provided in the MSA Code of Ethics, this Policy and the law.

It is strictly forbidden for peer-workers, trustees 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

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.

Peer-workers, trustees 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 peer-workers, trustees 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 MSA and MMO 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 MSA and its MMO's 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.

7. Breaches of Confidentiality

¹ The Privacy Officer for MSA is the Chair of the Ethics and Standards Committee or his Nominee; The Privacy Officer for an MMO is the Manager

The New Zealand Privacy legislation was updated in November 2020.

Under the revised legislation, MSA, or an MMO is required to notify the Privacy Commissioner and the affected individual(s) as soon as practicable after becoming aware of a notifiable privacy breach. A notifiable privacy breach means a breach that has caused serious harm to an affected individual or is likely to do so

The Act sets out a non-exhaustive list of factors to consider when deciding if a privacy breach is likely to cause serious harm but stops short of actually defining “serious harm”. It is important to err on the side of caution in complying with the legislation. Accordingly, any breach of privacy involving the unauthorised access of client information by any person or persons shall be regarded as having the potential for ‘serious harm’. However, there is a need to exercise some discretion in deciding if the breach is serious enough to notify the Commissioner.

When a notifiable breach occurs, under certain circumstances MSA, or an MMO, may also provide an affected individual with details of any person or body in possession of their information.

MSA or an MMO may pass on these details if there are reasonable grounds to believe that identification was necessary prevent or lessen a serious threat to an individual’s life or health.

MSA or MMO employees are not personally liable for delays in notifying an affected person of a notifiable privacy breach. However, responsible MSA or MMO Trustees remains liable.

MSA or an MMO may delay notifying individuals or the public if the notification itself would risk further breaches – for example, if this would make others aware of the method used to access the information. MSA, or an MMO, would still be required to notify the Commissioner as soon as practicable.

MSA or an MMO may also decide not to inform an individual of a breach if informing them would be likely to prejudice the individual’s health, or the individual is under 16 years of age and MSA, or an MMO, believes notification is not in their best interests.

Managing a privacy breach involving unauthorised access to client information should follow the following process:

- Ascertain the nature and extent of the breach and determine the causal factors.
- Inform the MSA or MMO Chair and Privacy Officer of the nature and extent of the breach and determine if:
 - o any notification exemptions apply,
 - o the client needs to be notified of the individual(s) or organisation that has accessed their information.
- Notify the client of the breach including details of the information accessed, and where appropriate, who accessed the information.
- Determine what changes in policies, procedures or systems are necessary to address the breach and ensure that confidential client information remains secure.
- Notify the Commissioner of the nature and extent of the breach, the information communicated to affected clients and the action taken to secure confidential client information.
- Prepare a report to the Board that documents the nature and extent of the breach, the actions taken to notify clients and the Commissioner, the client impacts of the breach and any resultant policy, procedure or system changes made to prevent a recurrence.

