Privacy – Information Security, Governance and Data Breach Policy

SCOPE: This policy applies to all employees, participants, participant representatives, Board members, volunteers, contractors, visitors, and students of The Onemda Association.

POLICY: Onemda respects the privacy of all associated with the Onemda service, and is committed to safeguarding rights in regards to privacy.

The Onemda Association respects and upholds the right to privacy protection under the Australian Privacy Act (1988), and the Victorian legislation – Privacy and Data Protection Act (2014) and Health Records Act (2001) in regulating how we collect, use, store, disclose and dispose personal information. As well as the Notifiable Data Breach Scheme in how Onemda responds to breaches.

Further to this there are other governing frameworks Onemda needs to operate in line with, this includes but not limited to:

- Australian Privacy Principles (APP)
- Information Privacy Principles (IPP)
- Victorian Protective Data Security Standards (VPDSS)

The aim of this policy is to:

- Provide the expectations and safeguarding procedures of personal information handling practices.
- Empower all stakeholders with the understanding of how personal information is utilised and the safeguards required in this process.
- How any breaches will be investigated and reported.
- Allow employees to information essential to performing their role.

Privacy- Information Security, Governance and Data Breach Procedure

Supporting Onemda frameworks and governance

Human Resource practices will support the frameworks of privacy, confidentiality and information security.

Onemda will operate a governance structure of access and information security, this will be formalised in - The Onemda Association – Manual of Delegations. *(however titled).*

In the context of risk mitigation and continuous organisational improvement, Onemda will have Information Security as part of its risk assessment, management and planning processes.

IT security controls will be implemented, appropriately monitored, reviewed and updated. Onemda will engage an external IT company to assist in ensure IT protection. Onemda will monitor and review its IT security with its IT provider annually.

Onemda will have its Privacy – Information security, governance and data breach policy publically available.

What information falls under the legislated and governing frameworks?

Personal information as defined by the Privacy Act 1988 (as amended) is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not.

Sensitive information as defined by the Privacy Act 1988 (as amended) is information or opinion (that is also personal information) about an individual's health, disability, racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or criminal record or health, genetic, biometric information or biometric templates.

Other information: Onemda uses the information for function or activity. Including, but not limited to, to deliver tailored services, banking details for wages or debiting fees, tax file number for taxation, personal contact details for emergency purposes.

Onemda context

Personal and sensitive information, is only collected as is necessary for a function or activity. To enable Onemda to carry out its work and deliver services to the participant or participant representatives, or its employer functions.

Non client specific information, may also be collected, including but not limited to commercial and legal information – agreements and contracts or financial information.

Participants or participant representatives may decide that they would prefer to not provide Onemda with such information. They may also choose to change this information at any time or access their personal file. Individuals also may opt out of providing personal information. They may also use a pseudonym or be de-identified.

Onemda will collect, store, use, disclose and dispose such information in a non-intrusive, lawful and fair manner. Confidential information may be either personal or sensitive information.

Handling Confidential Information

Confidential information may only be collected, accessed and used for a valid work purpose. When handling confidential information:

- Confirm details before sending faxes or emails
- Hard copies of confidential information kept securely
- Be aware of surroundings and people nearby

- Limit taking hard copy information away from secure sites
- Secure information when travelling eg: briefcase
- Dispose correctly
- Ensure that information is available to people who need access to it.
- Confidential, sensitive or personal information is not to be kept on hard drives.

Sharing confidential information

Any request to staff from government bodies or external organisations for information regarding participants must be checked and approved by the Senior Management before it is released in line with legislation.

Confidential information may be shared only:

- when a formal agreement exists in relation to information or data sharing between parties
- in circumstances permitted under Privacy Legislation. eg: Court orders.
- Consent is gained from the person or person's representative to share.
- There is protection of any sensitive information about an unintended person.

Images or information about participants is not to be shared with members of the public or at public forums without the consent of Senior Management. Senior Management are to ensure that they gain written consent from the participant or as appropriate the authorised participant representative, which in most cases will be primary carers or designated persons under Guardianship and Administration rulings. If there is ambiguity, in relation to consent Onemda will seek advice from the Office of the Public Advocate. In circumstances where written consent is not possible, verbal consent may be sought. The Manager is to make client file notes as appropriate, noting who gave consent, what the consent was for, and date.

Images of participants, including uploading of newsletters, may be posted on Onemda's website from time to time. Only images that are appropriate, respectful and have prior consent will be utilised.

All Onemda employees, volunteers and contractors are to maintain confidentiality regarding any information gained through their work and not divulge personal information of participants or staff.

If staff are allowed access to Senior Management computers, files or diaries, they are to remain at the task that permission was granted for. Inappropriate searching in computers, files or diaries can result in a Performance Management process being undertaken. Onemda applies access delegated passwords on IT systems.

When accessing client information, via an online medium, this is to be done during business hours. When sending confidential information via an online medium, attach the information with appropriate protection. Do not send confidential information in the subject line. Do not send confidential information to or from a free web-based email account.

Cloud storage

The use of cloud storage (and alike) must be for work purposes and in line with this policy and Professional conduct policy. Access must be authorised and must remain in the scope of your assigned role and task. Information on cloud storage systems should not be saved as a

'screen shot' or photographed (or alike) except with appropriate levels of authorisation for an authorised purpose.

Employees must not share log-in credentials with co-workers or others. Access outside working hours is not permitted. All access is time stamped. On cessation of employment the systems manager will remove access.

Passwords

Use identification and passwords to access computer services are for the sole use of the person to whom they are allocated.

Downloading software and suspicious emails

Software, emails and applications downloaded from the Internet can contain viruses that threaten the security of information stored on users' computers. Do not open emails from unknown senders or download unauthorised software.

Physical Security and Conversation

Onemda will take reasonable steps to ensure:

- Clear desks and screens
- Maintain an environment clear of sensitive information when unattended.
- Being mindful when conversing with others

Information disposal

Ensure record retention requirements have been met prior to the disposal of any business information.

When disposing of confidential information:

- Place unneeded working documents or copies of information in secure bins or adequate shredders.
- Ensure any electronic media including computers, hard drives, USB keys etc are sanitised when no longer required.

Portable Storage Devices (including usb, mobile phones)

Portable storage devices are usually small and capable of storing large amounts of information, and in some cases can be used to copy, transmit or share information.

Using portable storage devices to access, store or transport confidential information involves considerable risk because:

- they can be easily lost or stolen, and then accessed by unauthorised people
- using portable storage devices in public or non-agency premises increases the chance of accidentally disclosing confidential information to unauthorised people.

To minimise the information security risks associated with using portable storage devices:

- only use encrypted portable storage devices to store confidential information
- avoid storing confidential information on portable storage devices, where possible
- secure portable storage devices when unattended e.g. lock in a drawer
- report lost or stolen portable storage devices immediately to your manager

Personal storage devices (including personal mobile phones)

- Onemda acknowledges that the ability to have photographs taken and information stored of the participants is of tremendous benefit to participants. It is also mindful of the challenges it presents.
- Information/images should be transferred to Onemda's computer as quickly as practicable, preferably that day, and then deleted and should not be saved on an unauthorised external computer.
- Information or images of participants kept on personal devices should be kept securely and password protected. This information or images should not be shared with any unauthorised person and importantly should not be shared with people outside the Onemda community.

Data Breached and Incident Reporting

It is vital to report to senior managers all potential incidents as soon as possible so that their impact may be minimised.

- Staff should be aware of:
  - how to identify potential security incidents
  - the reason for reporting incidents is so their impact can be minimised—it is not to punish individuals
  - the need to report all incidents to their manager as soon as they become aware of them.
- Management can use the Onemda's Privacy & Confidentiality Breach Checklist
- Depending on the level or potential impact of the Breach, it may be necessary to report under the **Notifiable Data Breach Scheme**. – See the Office of the Australian Information Commissioner for details. Further to this, a DHHS incident report process may be required or reporting to the Office of the Privacy Commissioner.

Any request to staff from government bodies or external organisations for information regarding participants must be checked and approved by Senior Management before it is released in line with legislation.

Related references and links

Disability Act

Office of the Aust. Information Commissioner - Privacy Act

Commission for Privacy and Data protection- Victoria

Notifiable Data Breach Scheme