Privacy Policy

1. Commencement and application of this Policy

1.1 This Privacy Policy ('Policy') commences operation from 1 April 2020 and replaces all previous Manning Support Services Inc. (MSS) policies pertaining to privacy.

1.2 The Policy applies to all employees, agents and contractors (including temporary contractors) of MSS, collectively referred to as 'workplace participants'.

1.3 The Policy does not form part of any employee's contract of employment. Nor does it form part of any other workplace participant's contract for services.

1.4 MSS reserves the right to vary, replace or terminate this Policy from time to time.

2. MSS respects privacy

2.1 All employees of MSS may be exposed to information which is confidential and/or privileged and proprietary in nature. Respecting the privacy of our clients, members and employees of MSS is a basic value of MSS. It is the policy of MSS that such information must be kept confidential both during and after employment.

2.2 Confidential information includes client, employee, volunteer information and intellectual property of MSS that is covered in the MSS confidentiality agreement. Intellectual Property (IP) is a broad term encompassing written, graphic and audio-visual material. Under Australian law, IP of work created by paid employees is owned by their employer. IP also includes service / program information, policies and procedures, organisational forms and documentation which have been created by MSS employees.

2.3 It is a requirement that:

a) All employees are to take reasonable steps to maintain the security of confidential information including but not limited to, maintaining the physical security of confidential information by locking drawers and filing cabinets, and use of computer passwords;

b) Care be taken to ensure that unauthorised individuals do not overhear any discussion of confidential information and that documents containing confidential information are kept in a manner to prevent access by unauthorised people;

c) When destroying confidential information and/or organisational and client records, information is required to be placed in the destruction bins; and

d) All employees sign the confidentiality agreement upon commencement with MSS and are responsible to abide by this agreement.

3. Collection of Information

3.1 Personal information that would allow us to identify a named individual or contact them is collected only when knowingly and voluntarily submitted. For example, we may need to collect such information to provide you with further services or to answer or forward any requests or enquiries. Personal information we may collect includes but is not limited to:

a) Name;
b) Address;
c) Email address;
d) Date of birth;
e) Gender;
f) Mobile phone number; and/or
g) Drivers Licence number.

3.2 Sensitive information is a special category of personal information and includes, but is not limited to information about;

a) Health;
b) Race or ethnic origin;
c) Political or religious beliefs; and/or
d) Criminal record.

3.3 MSS may collect personal information through a variety of channels including:

a) Client contact via phone call;
b) Client interview for provision of service; or
c) Recruitment process.

3.4 Personal information collected by MSS is used only for the purpose for which it is provided to us unless we disclose other uses in this Privacy Policy or at the time of collection. We may collect personal information for the following purposes:

a) Record keeping and back-up purposes;
b) Marketing purposes;
c) Analysis of statistical data to improve our services or develop new services;
d) Analysis of statistical data for financial modelling purposes or to asses the profitability or otherwise of the services; or

e) To maximise the safety of our clients and workers.

4. Accessing and Correcting Information

4.1 Anyone has the right under the Privacy Act to ask MSS for access to information that we hold about them. There is no fee for asking for access, but we can charge a reasonable fee for retrieving and providing information. MSS may ask a requester to establish their identity before providing information. In some cases the law allows MSS not to disclose information. For further information please refer to the Privacy Act 1998 (Cth) for further information.

4.2 Anyone can also request that information MSS holds about them is corrected if they think it is incorrect or not up-to-date. If we agree that the information should be corrected, we will do so without charge. If we don't agree that the information should be corrected, the requester can ask us to include a note that they do not think the information is accurate. This is part of MSS's commitment to take all reasonable steps to ensure that the information we hold about clients, workers, and other stakeholders is accurate, complete and up-to-date.

4.3 If any party is concerned about MSS's handling of their personal information, they can submit details of their concern via email to ceo@mssinc.org.au. MSS takes complaints seriously and will endeavour to respond in writing within 30 days. We may need to contact the requester to obtain more information in order to investigate the matter to which the complaint relates.

5. Data Breach

5.1 The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

5.2 Accordingly, MSS needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes an NDB.

5.3 Adherence to this Procedure and Response Plan will ensure that MSS can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

6. Suspected Data Breach Process

6.1 **Alert** - Where a privacy data breach is known to have occurred (or is suspected) any member of MSS staff who becomes aware of this must, within 24 hours, alert the CEO or a member of the Executive in the first instance. The Data Breach Process Form should be used and the information provided (if known) should include:

a) When the breach occurred (time and date);

b) Description of the breach (type of personal information involved);

c) Cause of the breach (if known) otherwise how it was discovered;

d) Which system(s) if any are affected;

e) Which team is involved; and

f) Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

6.2 **Assess and determine potential impact –** Once notified of the information above, the CEO or a member of the Executive must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity.

6.2.1. Criteria for determining whether a privacy data breach has occurred:

a) Is personal information involved?

b) Is the personal information of a sensitive nature?

c) Has there been unauthorised access to personal information, or unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

6.2.2. Criteria for determining severity:

a) The type and extent of personal information involved.

b) Whether multiple individuals have been affected.

c) Whether the information is protected by any security measures (password protection or encryption).

d) The person or kinds of people who now have access.

e) Whether there is (or could there be) a real risk of serious harm to the affected individuals (serious harm could include physical, physiological, emotional, economic / financial or harm to reputation and is defined in section 9 of the Privacy Policy and section 26WG of the NDB Act).

f) Whether there could be media or stakeholder attention as a result of the breach or suspect breach.

6.3 **Action to be taken** - Within 24 hours of being notified, the CEO or member of the Executive must:

a) Immediately contain the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.

b) Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach having regard for the information outlined in sections 6.2.1 and 6.2.2 above.

c) Call upon the expertise of, or consult with, relevant staff in the particular circumstances.

d) Engage an independent cyber security or forensic expert as appropriate.

e) Assess whether serious harm is likely (with reference to section 6.2.2 above and section 26WG of the NDB Act).

f) Establish whether this breach constitutes an NDB for the purpose of mandatory reporting to the OAIC and the practicality of notifying affected individuals.

g) Consider developing a communication or media strategy including the timing, content and method of any announcements to students, staff or the media.

6.4 **Notification** – If the CEO or member of the Executive determines that there are reasonable grounds to suspect that an NDB has occurred, a prescribed statement must be prepared and a copy provided to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach). The Notifiable Data Breach Statement Form should be completed for this step. If practical, MSS must also notify each individual to whom the relevant personal information relates. Where impracticable, MSS must take reasonable steps to publicise the statement (including publishing on the website).

7. Breaches of this Policy

7.1 A failure to comply with the obligations contained in this Policy will lead to disciplinary action which may include, but is not limited to, termination of an employee's employment or a contractor's services.

7.2 Breaches of this Policy will be handled under MSS's Disciplinary Policy.

8. Variations

8.1 MSS reserves the right to vary, replace or terminate this policy from time to time.

Associated Legislation

- The Office of the Australian Information Commissioner's "Data breach notification guide: a guide to handling personal information security breaches"
- The Office of the Australian Information Commissioner's "Guide to developing a data breach response plan"
- Privacy Act 1998 (Cth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017

Associated Documents

- Code of Conduct
- Data Breach Process Form
- Notifiable Data Breach Statement Form

Policy version and revision information

Policy Authorised by: Board	Original issue: 07.05.2020
Policy Maintained by: CEO	Current version: 1
Review date: 26.03.2023	Latest issue: 07.05.2020

Workplace participant acknowledgement

I acknowledge that:

- *I have read this Policy;*
- *I must comply with the Policy; and*
- *There may be disciplinary consequences if I fail to comply with the Policy, which may result in the termination of my employment or contract for services.*

Workplace participant name: _____

Signed: _____

Date: _____