

# Code of Conduct

**Version 001**  
**Approved December 2021**

**Version 002**  
**Approved April 2023**  
**Review 2025**

## 1. Purpose

This policy outlines the required conduct at Mental Health First Aid (MHFA).

## 2. Scope and Application

This policy applies to all employees, volunteers and consultants.

This policy applies to all activities in connection with the work of MHFA, including but not limited to;

- work within the workplace
- work related activities outside the workplace
- work related events (e.g. social functions and conferences)
- work related interactions with customers, visitors, job applicants, trainers, instructors, the general public, MHFA employees and service providers.

## 3. Policy Statement

This policy covers the following:

3.1 General Conduct	p.1
3.2 Conflict of Interest	p.3
3.3 Acceptable use of Technology	p.4
3.4 Social Media	p.6
3.5 Intellectual Property	p.7
3.6 Confidential Information	p.7

### 3.1 General Conduct

**3.1 a** All behaviour and actions will be consistent with the MHFA values, namely being;

- Accountability
- Collaboration
- Creativity
- Empathy
- Inclusivity, and
- Integrity

**3.1 b** At all times employees, volunteers and consultants will:

- Act and maintain a high standard of integrity and professionalism.
- Perform duties with skill, honesty, care and diligence.
- Exercise fairness, equality, courtesy, consideration and sensitivity in dealing with all parties
- Maintain a cooperative and collaborative approach to working relationships.
- Use factual information to understand the strategic, financial and other implications of any decision making.
- Act in a financially responsible manner by seeking to understand and diligently carry out financial responsibilities.
- Be responsible in the proper use of MHFA information, equipment and facilities.
- Ensure that gifts or favours that may cast doubt on the recipient's ability to apply independent judgement as a representative of MHFA, are neither offered nor received.
- Be considerate and respectful of the environment.
- Promote the interests of MHFA.
- Strive to earn and sustain stakeholder trust at a high level.
- Abide by all MHFA policies, protocols, procedures and lawful directions.
- Comply with all relevant legislation and regulations in the execution of their work and in conducting work related activities.

## **3.2 Conflict of Interest**

### **3.2 a Conflict of Interest**

A conflict of interest arises whenever personal, professional or business interests are potentially at odds with the best interests of MHFA.

All parties are required to act in good faith towards MHFA. All parties must be aware of the potential for a conflict of interest to arise and should always act in the best interests of MHFA.

### **3.2 b Other employment or external interests**

All parties must disclose any other employment or private business activity that might cause a conflict of interest with MHFA to their manager. Where there are external involvements that do not represent a conflict of interest, these must not affect performance nor attendance whilst working at MHFA. If such involvement does affect performance or attendance it will be considered a conflict of interest.

### **3.2c Business or employment in competition with MHFA**

All parties must not set up or engage in private business or undertake other employment in direct or indirect competition with MHFA using knowledge and/or materials gained during the course of employment with MHFA.

### **3.2d Declare if in doubt**

It is impossible to define all potential areas of conflict of interest. If a party is in doubt if a conflict exists, the matter must be declared to their Director (or for Directors, to the CEO).

### **3.2 e Disclosure**

All parties must:

- disclose any potential, actual or perceived conflicts of interest (direct or indirect) that exist on becoming engaged by MHFA to management.
- disclose any potential, actual or perceived conflicts of interest (direct or indirect) that arise or are likely to arise during engagement by MHFA to management.
- avoid being placed in a situation where there is potential, actual or perceived conflicts of interest if at all possible.

### **3.2f Resolution of conflict of interest matters**

MHFA may require you to take action to eliminate or reduce any conflict of interest. In the event that, in the opinion of the MHFA, you fail or refuse to declare any such conflict, or to resolve it in a manner satisfactory to MHFA in accordance with its directions, this will be deemed to be a breach of this policy.

## **3.3 Acceptable Use of Technology**

### **3.3a Internet & Email**

#### **(i) Primary Purpose**

Access to the Internet and email is provided to allow for the execution of duties required to meet the business needs of MHFA.

#### **(ii) Limited personal use**

Limited personal use of the Internet and email is acceptable provided it complies with this policy and does not interfere with the work of the individual, the broader MHFA Australia team or MHFA's interests.

#### **(iii) Access, monitoring and blocking**

MHFA has the right to access incoming and outgoing email messages to check if an individual's usage or involvement is excessive or inappropriate.

MHFA Australia reserves the right to block emails or websites if they are considered to be offensive, illegal or defamatory. Receipt of any such messages must be reported to management immediately.

### **3.3 b Unacceptable use**

#### **(i) Email and Internet**

Unacceptable use of email and Internet by staff includes, but is not limited to:

- Creating or exchanging messages that are defamatory, offensive, harassing, obscene or threatening.
- Visiting websites containing objectionable (including pornographic) or criminal material.
- Exchanging confidential or sensitive information held by MHFA Australia (unless in the authorised course of their duties).
- Creating, storing or exchanging information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies).
- Creating or exchanging material that is prejudicial to the good standing of MHFA in the community or to its relationship with staff, customers, suppliers and any other person or business with whom it has a relationship.
- Internet-enabled activities such as gambling, gaming, conducting a business or conducting illegal activities.
- Creating or exchanging advertisements, solicitations, chain letters and other unsolicited or bulk email.
- Using another individual's account to send emails or access the internet unless given explicit permission from their supervisor.
- Using a private email address as an alternative to their work email address or automatically forwarding email messages from personal email accounts to their MHFA email address.
- Subscribing to social networking sites unless they have been given approval to do so in a work capacity.

#### **(ii) File streaming, downloading and uploading**

- Downloading and/or uploading files (e.g. video, music and other material) from the Internet is prohibited unless it is work related.
- Software files should not be downloaded without review and approval from MHFA Technology Team staff.

### **3.3c File management & sharing**

All files must be stored in designated directories (eg Sharepoint) on the network and/or

share drives. Files must not be saved on to local desktops.

### **3.3d Equipment for work related purposes only**

Any device or computer, including but not limited to, desk phones, mobile phones, tablets, laptops, desktop computers that MHFA Australia provides to staff, must be used for work related purposes only.

### **3.3e Technology Security**

Staff must maintain the security of MHFA information by:

- Keeping passwords confidential and using a OnePassword to store all work-related passwords.
- Logging out of workstations and/or remote connections when not in use.
- Immediately reporting lost or stolen equipment.

### **3.3f Access, Monitoring and Ownership of Technology**

- a) All staff, volunteers and consultants must be aware that:
- MHFA may monitor the use and access to email, chat messaging, Internet and computer facilities.
  - All information created and stored on MHFA equipment and accounts is the property of MHFA Australia.
  - MHFA may access emails sent or received by you, and monitor your electronic communications, from time to time for the purposes of conducting its business (including auditing compliance with this or any other Policy) or complying with its legal obligations. This may, for example, involve examining logs of your electronic communications activity, accessing emails you send or receive, including personal communications and examining your Internet browsing records. Only persons authorised by the CEO will be permitted to access your electronic communications.
- b) Authorised Technology staff may access employee technology accounts when they are requested to attend to a fault, upgrade or such similar situation. Access in this case will be limited to the minimum needed to address the task.

### **3.3g Failure to comply with acceptable Use of Technology**

Failure to comply with the Acceptable Technology Use provisions outlined in this policy (section 3.3) will constitute a breach of policy. All parties must be aware that some forms of Internet conduct may lead to criminal prosecution.

## **3.4 Social Media**

### **3.4a Professional Use of Social Media**

MHFA Australia embraces the use of social media for the promotion of mental health first aid and our courses, support of Instructors and MHFAiders and other activities relevant to the organisation. MHFA Australia recognises that all employees, volunteers and consultants can communicate online in many ways, such as through social media, professional networking sites, blogs, online news sites and personal websites. However, all need to use good judgment about what material appears online, and in what context.

‘Professional use’ applies to the official use of social media, where employees, volunteers and consultants have been authorised by MHFA Australia to use social media as a communication tool, to engage with the community, or to distribute content on behalf of the organisation. This includes posting to an official MHFA social media account, or commenting or posting as a MHFA representative on another organisation or person’s page (for example, posting an MHFA related message on Beyond Blue’s Facebook page).

Employees, volunteers and consultants conducting official communication through social media:

- Must have prior approval from the CEO or a Director to use social media in an official capacity.
- Must act in a professional manner at all times, and in the best interests of MHFA Australia.
- Should identify themselves as affiliated with MHFA Australia by using “MHFA” after their name when posting (e.g. Jane\_MHFA)
- Must avoid any statement that might bring MHFA Australia into disrepute.
- Must not commit MHFA Australia to any action or initiative without appropriate authority.
- Must not disclose information about MHFA Australia’s plans or operations unless authorised to do so.
- Must protect personal information entrusted to MHFA Australia from distribution into the public domain
- Must protect information (regardless of whether it is confidential or public knowledge), about clients, business partners or suppliers of MHFA Australia without their prior authorisation or approval to do so.
- Must take note of any copyright/Creative Commons notices attached to content they wish to use/repurpose and acknowledge content sources when they are known.
- Must refer to and follow the MHFA Australia Crisis Protocol for crisis communications.
- Must be in line with MHFA Australia’s social media guidelines as developed and amended from time to time

### **3.4 b Personal use of social media**

MHFA Australia recognises that those covered by this policy may wish to use personal social media accounts to talk about MHFA Australia. This policy does not intend to discourage nor unduly limit the personal expression of online activities. However, there is a risk that inappropriate behaviour on such sites could cause damage to MHFA Australia, especially when the user can be identified as an employee, volunteer or consultant of MHFA Australia.

Personal communications should not indicate that an employee, volunteer or consultant is speaking on behalf of MHFA Australia, and their social media name, handle or URL should not include MHFA Australia’s name or logo.

Employees and consultants of MHFA Australia, posting in a personal capacity must refrain from posting or promoting material that:

- is intended to (or could possibly) cause insult, offence, intimidation or humiliation to MHFA Australia, including employees, consultants, Instructors, MHFAiders, partners or the general public;
- is defamatory or could adversely affect the image, reputation, viability or profitability of MHFA Australia, or
- contains any private staff or customer information
- contains any form of confidential information relating to MHFA Australia.

### **3.5 Intellectual Property**

All employees acknowledge and agree that it is a condition of their employment that MHFA shall be the owner of all Intellectual Property (IP) Rights in everything developed, created, generated or contributed to in the course of their employment or arising out of employment with Mental Health First Aid Australia, whether alone or in conjunction with others, and whether during or outside working hours.

### **3.6 Confidential Information**

#### **3.6a Privacy Policy**

Employees, volunteers and consultants must have read and understood the MHFA Privacy Policy before working with any confidential information.

#### **3.6b Non-disclosure agreement**

All consultants and volunteers must sign a non-disclosure agreement prior to dealing with any confidential information.

#### **3.6c Management of Confidential Information**

Employees, volunteers and consultants must act in good faith towards MHFA and must prevent (or if impractical, report) the unauthorised disclosure of any confidential information.

Employees, volunteers and consultants must not (during or after their engagement) with MHFA:

- disclose or use any part of any confidential information outside of the performance of their duties; or
- authorise or be involved in the improper use or disclosure of confidential information

## **4. Definitions**

### **Conflict of Interest**

Conflict of interest arises whenever the personal, professional or business interests of an employee are potentially at odds with the best interests of MHFA.

### **Confidential Information**

'Confidential information' includes any information in any form relating to MHFA and related bodies, clients or businesses, which is not in the public domain.

### **Social Media**

Forms of social media include, but are not limited to, social or business networking sites (i.e. Facebook, LinkedIn), video and/or photo sharing websites (i.e. YouTube, Instagram), business/corporate and personal blogs, micro-blogs (i.e. Twitter), chat rooms and forums.

## 5. Responsibilities

<p><b>Employees, Volunteers, Consultants</b></p>	<p><b>All employees, volunteers and consultants will:</b></p> <ul style="list-style-type: none"> <li>• Read, understand and abide by this policy</li> <li>• Disclose any activity that they become aware of that is not in accordance with this policy.</li> </ul>
<p><b>Managers and Supervisors</b></p>	<p><b>Managers and Supervisors will:</b></p> <ul style="list-style-type: none"> <li>• Ensure that all staff, volunteers and consultants are provided with a copy of or access to this policy.</li> <li>• Ensure all activity within their remit is conducted in accordance with this policy.</li> <li>• Role model the Code of Conduct.</li> </ul>
<p><b>Chief Executive Officer (CEO)</b></p>	<p><b>The Chief Executive Officer will:</b></p> <ul style="list-style-type: none"> <li>• Be accountable for the implementation and execution of this policy.</li> <li>• Provide guidance on the application of this policy, as and when required.</li> <li>• Ensure breaches of this policy are investigated.</li> <li>• Initiate changes to this policy, as and when required.</li> <li>• Escalate any significant strategic or operational risks to the Board and Audit &amp; Risk Committee.</li> <li>• Role model the Code of Conduct.</li> <li>• Monitor the application of this policy and its impact.</li> <li>• Recommend changes to this policy to the Board.</li> </ul>
<p><b>Audit &amp; Risk Committee (A&amp;RC)</b></p>	<p><b>The A&amp;RC will:</b></p> <ul style="list-style-type: none"> <li>• Role model the Code of Conduct.</li> <li>• Report to the Board on the effectiveness of the Code of Conduct policy.</li> </ul>
<p><b>Board</b></p>	<p><b>The Board will:</b></p> <ul style="list-style-type: none"> <li>• Role model the Code of Conduct</li> <li>• Receive advice from the A&amp;RC on the effectiveness of the Code of Conduct.</li> <li>• Review and change this policy as required, based on advice from management and the A&amp;RC.</li> </ul>

## 6. Compliance

### 6.1 Breach of Policy

Any breach of this Policy will be treated as a serious matter and may result in disciplinary action including termination of employment, termination of volunteering arrangements or (for contractors and sub-contractors) the termination or non-renewal of contractual arrangements. Other disciplinary action



that may be taken includes, but is not limited to, issuing a formal warning, directing people to attend mandatory training, suspension from the workplace and/or permanently or temporarily denying access to all or part of MHFA's operations. All parties must be aware that any breach of this Policy that is unlawful, may also result in legal action and/or criminal prosecution.

## **6.2 Whistle-blower Protection**

Any individual, who in good faith, discloses an alleged breach of the Code of Conduct, will not be disadvantaged or prejudiced. Any disclosure in regard to an alleged breach of the Code of Conduct must be immediately reported to the CEO. In the case of a matter involving the CEO, the Board Chair must be advised immediately. All disclosures will be investigated in a timely and confidential manner.

## **7. Policy Owner**

The CEO is accountable for this policy. For inquiries about this policy, contact Human Resources.

## **8. Scheduled Review Date**

This policy is to be reviewed within 2 years from the date of approval.

## **9. Related Documents**

- Delegations of Authority Policy
- Equity & Diversity Policy
- Employee Grievance Policy
- Health and Safety Policy
- Privacy Policy