



Code of Conduct

Version 3.1

Approved 9 January 2026

1. Purpose

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

2. Scope and Application

This policy applies to all MHFAI employees, Board Directors, non-director independent Committee members, volunteers and consultants (referred to in this Policy as **workplace participants**) and their conduct in the **workplace**.

In this Policy, **workplace** means all activities in connection with the work of MHFAI, including but not limited to:

- Work at MHFAI's premises;
- Related dealings for MHFAI outside MHFAI premises;
- Functions, conferences and events;
- Work-related travel;
- Electronic communications and social media, including out-of-hours communications; and
- Dealings with stakeholders, customers, visitors, job applicants, service providers and the public.

This policy covers the following main areas:

- General Conduct
- Conflict of Interest
- Acceptable use of Technology
- Social Media
- Intellectual Property
- Confidential Information

3. General Conduct

3.1 All behaviour and actions will be consistent with the MHFAI principles, namely:

- Agility
- Integrity
- Equity
- Collaboration
- Respect

3.2 At all times, workplace participants 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 MHFAI information, equipment and facilities.
- Ensure that gifts or favours that may cast doubt on the recipient's ability to apply independent judgement as representative of MHFAI, are neither offered to nor received from others.
- Be considerate and respectful of the office environment.
- Promote the interests of MHFAI.
- Strive to earn and sustain stakeholder trust at a high level.
- Abide by all MHFAI 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.

4. Conflict of Interest

4.1 Conflict of Interest

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

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

4.2 Other employment or external interests

All workplace participants must disclose any other employment or private business activity that might cause a conflict of interest with MHFAI to their manager, or, in the case of Board Directors and non-director independent Committee members, to be conducted in accordance with the Board Charter. Employees must seek the written consent of MHFAI before being employed or otherwise engaged by any other entity or in connection with any other business. Where there are external involvements that do not represent a conflict of interest, these must not affect performance nor attendance whilst working at MHFAI. If such involvement does affect performance or attendance, it will be considered a conflict of interest.

4.3 Business or employment in competition with MHFAI

Workplace participants must not set up or engage in private business or undertake other employment in direct or indirect competition with MHFAI using knowledge and/or materials gained during the course of employment or engagement with MHFAI.

4.4 Declare if in doubt

It is impossible to define all potential areas of conflict of interest. If a workplace participant is in doubt if a conflict exists, the matter must be declared to their Executive Director (or for Executive Directors, to the CEO). Board members and non-director independent Committee members should declare interests and potential conflicts to the Company Secretary and in accordance with the Board Charter.

4.5 Disclosure

All workplace participants must:

- disclose any potential, actual or perceived conflicts of interest (direct or indirect) that exist on becoming engaged by MHFAI to management, or in the case of Board Directors and non-director independent Committee members to the Company Secretary and in accordance with the Board Charter.
- disclose any potential, actual or perceived conflicts of interest (direct or indirect) that arise or are likely to arise during engagement by MHFAI to management, or in the case of Board Directors and non-director independent Committee members, to the Company Secretary and in accordance with the Board Charter.
- avoid being placed in a situation where there are potential, actual or perceived conflicts of interest if possible.

4.6 Resolution of conflict-of-interest matters

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

5. Acceptable Use of Technology

The provisions outlined in the following sections may not be relevant to all workplace participants. For instance, Board Directors and non-director independent Committee members are generally not issued an MHFAI email account, hardware, or access to operational systems. Exceptions may be made based on specific needs. Therefore, these clauses apply only insofar as they are relevant to the individual's role and circumstances.

5.1 Internet & Email

5.1.1 Primary Purpose

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

5.1.2 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 MHFAI team or MHFAI's interests. The use of MHFAI technology or devices for personal business use or other employment is prohibited.

5.1.3 Access, monitoring and blocking

Any communication on MHFAI devices belongs to MHFAI and is subject to scrutiny by the organisation. Storing MHFAI documentation on non-MHFAI devices is prohibited.

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

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

5.2 Unacceptable use

5.2.1 Email and Internet

Unacceptable use of MHFAI email and Internet by workplace participants 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 MHFAI (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 MHFAI 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 MHFAI email address.
- Subscribing to social networking sites unless they have been given approval to do so in a work capacity.

5.2.2 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 must not be downloaded without review and approval from MHFAI Technology Team staff.

5.3 File management & sharing

All files must be stored in designated directories (e.g. Sharepoint) on the network. Files must not be saved on personal devices.

5.4 Equipment for work related purposes only

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

5.5 Use of Personal Devices

Access to organisational applications and data via personal devices is strictly governed by the Information & Cyber Security Policy. Such access is authorised only where approved security controls are implemented and maintained in accordance with organisational standards.

5.6 Use of Large Language Models/Artificial Intelligence

The use of large language models/Artificial Intelligence is strictly governed by the Use of Artificial Intelligence Policy.

5.7 Technology Security

Workplace participants must maintain the security of MHFAI information by:

- Keeping all passwords confidential and storing all work-related passwords using 1Password (or other program as directed by MHFAI).
- Always logging out of workstations and/or remote connections when not in use.
- Immediately reporting lost or stolen equipment to the appropriate authority.
- Logging out of workstations and/or remote connections when not in use.

5.8 Access, Monitoring and Ownership of Technology

All workplace participants must be aware that:

- MHFAI may monitor the use and access to email, chat messaging, Internet and computer facilities.
- All information created and stored on MHFAI equipment and accounts is the property of MHFAI.
- MHFAI 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.

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.

5.9 Failure to comply with acceptable Use of Technology

Failure to comply with the Acceptable Technology Use provisions outlined in this policy (section 5) will constitute a breach of policy. All parties must be aware that some forms of Internet conduct may lead to criminal prosecution.

6. Social Media

6.1 Professional Use of Social Media

MHFAI 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.

MHFAI recognises that all workplace participants can communicate online in many ways, such as through social media, professional networking sites, blogs, online news sites and personal websites. However, all such communications that reference mental health first aid, or MHFAI must comply with the Social Media Protocol.

‘Professional use’ applies to the official use of social media, where workplace participants have been authorised by MHFAI 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 MHFAI social media account or commenting or posting as an MHFAI representative on another organisation or person’s page.

Workplace participants conducting official communication through social media:

- Must have prior approval from the CEO or an Executive Director to use social media in an official capacity. (Note that Board members or non-director independent committee members need prior approval from the Board Chair).
- Must act in a professional manner at all times, and in the best interests of MHFAI.
- Should identify themselves as affiliated with MHFAI by using “MHFAI” after their name when posting (e.g. Jane_MHFAI).
- Must avoid any statement that might bring MHFAI into disrepute.
- Must not commit MHFAI to any action or initiative without appropriate authority.
- Must not disclose information about MHFAI’s plans or operations unless authorised to do so.
- Must protect personal information entrusted to MHFAI 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 MHFAI 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 MHFAI Crisis Protocol for crisis communications.
- Must be in line with MHFAI’s social media guidelines.

6.2 Personal use of social media

MHFAI recognises that those covered by this policy may wish to use personal social media accounts to talk about MHFAI. 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 MHFAI, especially when the user can be identified as a workplace participant of MHFAI.

Personal communications should not indicate that a workplace participant is speaking on behalf of MHFAI, and their social media name, handle or URL should not include MHFAI’s name or logo.

Workplace participants of MHFAI, 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 MHFAI, including employees, consultants, Instructors, MHFAiders, partners or the general public;
- is defamatory or could adversely affect the image, reputation, viability or profitability of MHFAI;
- contains any private staff or customer information; or
- contains any form of confidential information relating to MHFAI.

7. Intellectual Property

All employees acknowledge and agree that it is a condition of their employment that MHFAI 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 International, whether alone or in conjunction with others, and whether during or outside working hours.

8. Confidential Information

8.1 Privacy Policy

Workplace participants must have read and understood the MHFAI Privacy Policy before working with any confidential information.

8.2 Deed of Non-Disclosure

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

8.3 Management of Confidential Information

Workplace participants must act in good faith towards MHFAI and must prevent (or if impractical, report) the unauthorised disclosure of any confidential information.

Workplace participants must not (during or after their engagement) with MHFAI:

- 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.

9. Definitions

Act in Good Faith

Acting in good faith means being honest, fair, reasonable, and to act with integrity.

Conflict of Interest

Conflict of interest arises whenever the personal, professional or business interests of a workplace participant are potentially at odds with the best interests of MHFAI.

Confidential Information

‘Confidential information’ includes any information in any form relating to MHFAI 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. X), chat rooms and forums.

10. Responsibilities

Board	The Board will: • Role model the Code of Conduct. • Review this Policy biennially or as circumstances require. • Receive recommendations from the GNRC on any proposed changes to the policy by the Committee or Management.
--------------	---

Governance, Nominations & Remuneration Committee (GNRC)	The GNRC will: • Role model the Code of Conduct. • Review the policy and make recommendations to the Board.
Chief Executive Officer (CEO)	The Chief Executive Officer will: • Provide guidance on the application of this policy, as and when required. • Ensure breaches of this policy are investigated. • Escalate any significant strategic or operational risks to the Board and Quality and Risk Committee. • Role model the Code of Conduct. • Recommend changes to this policy to the Board.
Executive Director Corporate Services	The Executive Director Corporate Services is: • Be accountable for the implementation and execution of this policy. • Monitor the application of this policy and its impact. • Initiate changes to this policy, as and when required. • Ensure that all workplace participants are provided with a copy of or access to this policy. • Role model the Code of Conduct.
Managers and Supervisors	Managers and Supervisors will: • Ensure all activity within their remit is conducted in accordance with this policy. • Role model the Code of Conduct.
Workplace Participants	All workplace participants will: • Read, understand and abide by this policy. • Disclose any activity that they become aware of that is not in accordance with this policy.

11. Compliance

11.1 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 MHFAI'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.

11.2 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 regarding an alleged breach of the Code of Conduct must be immediately reported to the CEO. In the case of a matter involving the CEO or a Board member, the Board Chair must be advised immediately. All disclosures will be investigated in a timely and confidential manner.

12. Policy Owner

The Executive Director Corporate Services is accountable for this policy. For inquiries about this policy, contact People and Culture.

13. Scheduled Review Date

This policy is to be reviewed within three (3) years from the date of approval.

14. Related Documents

- Delegations of Authority Policy
- Diversity, Equity & Inclusion Policy
- Employee Grievance and Dispute Resolution Policy
- Harassment, Bullying and Discrimination Prevention Policy
- Health and Safety Policy
- Information & Cyber Security Policy
- Privacy Policy
- Social Media Protocol
- Use of Artificial Intelligence Policy (in development)
- Whistleblower Policy

15. Document Controls

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest version.

Version

Document Name	Code of Conduct
Document Number	PO-0123
Status:	Approved
Approver:	Board
Reviewer:	GNRC
Directorate:	CS
Version No:	3.1
Date:	9 January 2026
Distribution:	This document may be publicly released
Review Period:	3 years
Next review by:	January 2029

Revision History

<i>Version</i>	<i>Date of Issue</i>	<i>Approved</i>	<i>Summary of changes</i>
001	December 2021	December 2021	New Policy
002	April 2023	April 2023	Biennial review
3.0	11 December 2025		Biennial review. Full review by Exec. Initial review by GNRC in August 2025. Further changes flowing from that meeting.
3.1	19 December 2025	9 January 2026	Review period changed from 2 years to 3 years approved by Board 11 Dec 2025. Further changes requested by Board on 11 Dec 2025 around BYOD