STAFF SAFETY AND SECURITY SUPPORT GUIDELINES (PSYCHOSOCIAL RISKS)

Section	Health, Safety & Wellbeing
Contact	DVC University Services
Last Review	September 2024
Next Review	September 2026
Effective from	September 2024

Introduction

The Staff Safety and Security Support Guidelines are designed to sit alongside the university's existing policies, in particular, the university's Academic Freedom Policy which takes a justice-based approach to the exercise of academic freedom. The Staff Safety and Security Support Guidelines are designed to support the safety and wellbeing of all staff.

A justice-based approach to supporting academic freedom recognises the broader context in which we operate, including acknowledging the history of Aotearoa New Zealand and the role of place, and paying attention to vulnerability, especially for historically marginalised groups. Furthermore a justice-based approach responds to the intersecting contexts of colonisation, racism, patriarchy, and cis-normativity and calls attention to the power imbalances that have historically silenced academic inquiry. It means attending to unequal power structures, reducing inequities and challenging unjust power and social relations

These Guidelines have been developed by the university in its efforts to take all reasonably practicable steps to ensure the elimination of harm (or minimisation where this is not possible) to workers and others associated with the university. Furthermore, where actual or potential harm is identified, the university will support staff in exercising academic freedom in response to staff being targeted by individuals and groups who use threats of harm and abuse to intimidate staff, their colleagues, and/or whānau with the aim being to deter and prevent staff member's academic voice.

Physical, psychological, social or cultural threats of harm on academic staff covered by these Guidelines need to be clearly recognised as unacceptable practices in situations where public or academic discourse can be reasonably recognised as normative disagreement or scholarly debate. These Guidelines are designed to assist management enquiry and response to ensure the safety of workers and others, and support staff where there is evidential indication of real or perceived threats of harms to the safety and wellbeing to staff (including colleagues and whānau), both on and off campus. These guidelines included anticipated and actual abuse and/or targeted campaigns of a political, ideological and organised nature.

Determination of Risk:

The Guidelines are specifically designed to ensure that workers and others are supported by appropriate university interventions and services when indications of evidential threats of harm, abuse and/or targeted campaigns of an ideological or political nature are present and where the staff members cultural, social, mental or physical health and/or bodily security, and/or that of their colleagues and/or whānau are deemed at risk.

Understanding management of risk exposure involves (1) identification of threats of harm, (2) assessment of risk consequence outcomes, (3) recognition of existing mitigation control effectiveness, and (4) review of future risk mitigations that ensures the elimination or minimisation of harm to workers and others.

© This Policy is the property of Massey University

Risks can be either internal or external to the university and may include:

(a) online or in person abuse or threats of harm

(b) digital disinformation campaigns

(c) disinformation distributed on mainstream media

(d) targeted campaigns directed at academics

(e) political pressures

(f) threat of lawsuits,

(g) the vexatious use of university processes, such as formal complaints processes or OIA requests, to reproduce and circulate disinformation targeting academics.

It is also noted that understanding management of risk exposure is not necessarily subject to any of these risk exposures emanating from New Zealand or undertaken by persons resident in New Zealand. It is understood that risk exposure can originate from outside New Zealand's borders.

Threat of Harm Categories *and* Guidelines for Managing Risk and Providing Support for Staff

Within this context these Guidelines aim to outline for staff the services available to them under different categories of threat of harm. It is recognised that the categories presented will not be exhaustive and, in some cases, will overlap. In each case there remains an expectation that affected staff would first liaise with their line manager who would provide advice, guidance, and support the staff member in accessing available university, and where applicable, external services. Additionally, the university will seek to understand the source of the threats of harm in order to improve control mitigations and systems necessary to eliminate the risk of harm to workers and others. The clarification of categories, identification of key university officers responsible for the provision of related services, and identification of the services themselves, are expected to provide staff and their managers with an understanding of what responses can be enacted and by whom.

1. Cyberbullying threats of harm

Cyberbullying can range from offensive or cruel online posts or digital pictures, to online threats, harassment, and negative comments, to stalking through emails, websites, social media platforms and text messages (https://staysafeonline.org/online-safety-privacy-basics/cyberbullying/). In a situation where a staff member feels they are subject to cyberbullying there are steps they can take:

i. Advise their line manager and provide evidence of the material in question
ii. Initiate safety protocol risk management procedures for the identification, assessment, control and review of the risk category as it affects the Occupational Health, Safety and Wellbeing Policy. Where necessary seek the advisory support of the Office of Occupational Health, Safety and Wellbeing.
iii. If there is agreement (seeking the advice of the Director Governance & Assurance, or Executive Director People & Culture in addition to the Chief Information Officer (CIO)) that the material is deemed to constitute cyberbullying the line manager would contact the Head of Security (IT) and provide details.
iv. The Head of Security (IT) would consider the information provided with the staff member and line manager and may:
    a. Deem that no action is warranted

© This Policy is the property of Massey University

b. Facilitate access to Netsafe, a free and confidential service to help people experiencing online bullying, abuse and harassment. Netsafe can also explain how the Harmful Digital Communications Act (HDCA) may apply to you as this law deals with image based abuse (like revenge porn), incitement to suicide and extremely offensive, abusive or harassing content (https://www.netsafe.org.nz/bullying-abuse-support/) and, depending upon outcome:
c. Apply for a harmful digital communication order through a District Court (https://www.justice.govt.nz/courts/civil/harmful-digital-communications/), and/or
d. Establish web, social media and email protocols that will effectively shield the staff member and other affected parties from the cyberbullying activity.

2. Online and traditional media threats of harm

Bullying via traditional and online media in a contemporary setting can be blurred given the often-seamless interaction between media types. This area is further complicated by social media within online and traditional media settings. As such details provided above under the cyberbullying heading are likely to be relevant in cases where staff are being unreasonably targeted via online and traditional media. As such similar processes should be followed. In addition, in situations where staff consider themselves to be the focus of unreasonable attacks from traditional or online media they should:

i. Advise their line manager and provide evidence of the material in question
ii. Initiate safety protocol risk management procedures for the identification, assessment, control and review of the risk category as it affects the Occupational Health, Safety and Wellbeing Policy. Where necessary seek the advisory support of the Office of Occupational Health, Safety and Wellbeing.
iii. If there is agreement that the material is deemed to fall within the remit of the staff safety and security guidelines the line manager would contact the CIO and/or the Executive Director Marketing and Communications (EDMC) and provide details.
iv. The CIO and/or EDMC, staff member and line manager would consider the information provided with the staff member and line manager and may:
    a. Deem that no action is warranted
    b. Implement steps b, c and/or d under 'cyberbullying' above
    c. Support a complaint to the New Zealand Media Council (https://www.mediacouncil.org.nz/)

3. Physical threats to personal safety and wellbeing

Physical threats and a concern for a staff member's personal safety can emanate from online, traditional media, or physical environments. In addition to the steps outlined above in response to cyberbullying or attacks via online or traditional media, physical threats, and concerns regarding personal safety, require further consideration and potentially action. In a situation where a staff member feels that they are subject to physical threats and that their personal safety is at risk, or that their colleagues and/or family's safety is at risk, there are steps they can take:

i. Advise their line manager and provide evidence and / or provide an outline of the threats and risk to personal safety
ii. Initiate safety protocol risk management procedures for the identification, assessment, control and review of the risk category as it affects the Occupational Health, Safety and Wellbeing Policy. Where necessary seek the advisory support of the Office of Occupational Health, Safety and Wellbeing.
iii. If there is agreement that there is a potential risk to personal safety the line manager would contact the Emergency and Security Lead.
iv. The Emergency and Security Lead would consider the information provided with the staff member and line manager and may:

© This Policy is the property of Massey University

a. Institute on-campus security protocols with the agreement of the staff member
b. Institute off-campus security measures that may be deemed reasonable with the agreement of the staff member. E.g. being escorted to and from the office after hours, having locked/swipe-card access to university office space, or a panic alarm fitted under workstation or desk.
c. Advise local police and provide a briefing to them for assessment and potential follow up actions
d. In any situation where a staff members physical safety may be at risk as part of any offshore activities a comprehensive security assessment would need to be undertaken, and associated actions agreed to with the staff member prior to any approval for travel being granted.

Other Services / Actions

i. Occupational Health Safety and Wellbeing
   a. Employee Assistance Programme (EAP) services are available to staff to help navigate issues at work or home and are there to support your general health and wellbeing https://masseyuni.sharepoint.com/sites/OccupationalHealthAndSafety/SitePages/Employee-Assistance-Programme.aspx
   b. Workplace safety includes physical, psychological and cultural risks. Workplace safety is about the nature of relationships between people, organisation and threats of harm that arise out of workplace activity. Massey contacts and resources can be located at https://masseyuni.sharepoint.com/sites/OccupationalHealthAndSafety
   c. Managers and workers of the university need to be familiar with the Occupational Health and Safety Management Framework. In particular the Standards for Workplace Preventative and Curative Care, and Hazards and Risk Management and Management of Change.

ii. People and Culture
   a. Executive Director P&C, Director ER & Advisory / Legal Counsel and HR Advisory team can provide advice and guidance https://masseyuni.sharepoint.com/sites/WorkingAtMassey/SitePages/Contact-HR.aspx

iii. Freedom of Information (FOI)
   a. Provide staff with information outlining FOI conditions and expectations with links to relevant policies and guidelines both internal and external https://www.justice.govt.nz/about/official-information-act-requests/

iv. Advocacy strategies and actions
Consider the implementation of advocacy strategies using internal and possibly external resources to counter domestic or international trolling and false claims in general that may be impacting upon staff members.

Related procedures / documents:

Academic Freedom Policy
Employee Support Services Policy
Harassment and Discrimination at Work Policy
Harassment and Discrimination Resolution Procedures
Health, Safety and Wellbeing Policy

© This Policy is the property of Massey University

Document Management Control:

Prepared by: Professor Giselle Byrnes, Ms Shelley Turner
Authorised by: Deputy Vice Chancellor University Services
Date issued: 30 September 2024
Last review: September 2024
Next review: September 2026

© This Policy is the property of Massey University