

Guidance for research organisations supporting researchers facing online harassment

This resource offers practical guidance for research organisations supporting staff targeted by online abuse from outside the institution, including cases where the harassment escalates offline.

It contains a pool of ideas to set up systems to deal with incidents of online harassment, and protect researchers from online harm. These 'building blocks' reflect existing approaches in New Zealand and international institutions, and recommendations from researchers who have experienced harassment.

If your institution does not have a dedicated staff support team with capacity to provide these services, identify staff across different departments who will liaise with each other to provide coordinated support.

Responding effectively

Preparing in advance for when incidents of harassment occur

Coordination

Establish a single point of contact for researchers experiencing harassment who can help them access a broad range of support services. Key responsibilities of a 'staff support specialist' include:

- Meet with the affected researcher as soon as possible to discuss what they are experiencing and provide **moral support**.
- Outline the services and resources that are available and make a plan with the researcher to help them regain a sense of control and access the support they need.
- Coordinate the institution's response and ensure plans have been followed through.
- Debrief at the conclusion of the response and collect feedback to refine processes. Assist staff who anticipate harassment to plan ahead and access proactive support.

Reporting

Create a **reporting form** and **risk assessment system** so that staff can provide appropriate support. Key information includes:



Nature of the harassment: Determine whether abusers are known to the researcher (either by name, or social media handle) and whether the harassment has followed them across platforms or offline. Identify any specific threats.



Evidence of harassment: Instruct the researcher (or someone they delegate) to screenshot or save abusive content before blocking perpetrators, and to attach posts, messages, and emails to the form, noting the date, time, platform, and usernames. Additional advice for recording evidence of digital harm is available from [Netsafe](#).

NOTE: Documenting harassment may be distressing for the researcher. Reporting forms should include contact information for staff who can help the researcher fill out the form and collect evidence of the abuse. Assistance with documenting any further abuse should be provided on an ongoing basis.



Others who may be at risk: Consider co-investigators, research group members, and students, including those from other institutions. Identify those working in close physical proximity, especially where the threat involves possible or actual onsite harassment.

NOTE: Trained staff within the research organisation should cross-check assessments of who else may be at risk.



Demographic factors: The researcher's ethnicity, age, gender, sexuality, and subject area may influence how likely it is that the harassment will escalate.

TIP: Reports of abuse can also help institutions track the quantity and nature of harassment faced by their researchers.

Security

Establish security protocols to ensure the researcher's safety, such as:



Temporary relocation of classrooms and/ or office spaces



Change public access arrangements to buildings



Escort staff around campus and/or to and from cars



Trespass orders










Advice on home security and other precautions, such as changing travel routes to and from work

TIP: Security personnel should coordinate with staff monitoring ongoing abuse to conduct continuous risk assessments and respond accordingly.

Digital technology






Establish security protocols to ensure the researcher's safety, such as:

Some examples of actions that may be appropriate, depending on circumstances:

-  Remove sensitive information, contact details, and classroom / office locations from institutional websites, directories, and public-facing course materials.
-  Support the researcher to review their online footprint beyond institutional sites.
-  Block perpetrators from your research organisation's email and phone systems.
-  Create mailbox filters or proxies to intercept, monitor and document potentially abusive emails, or have the researcher forward them to a dedicated email address.
-  Set up auto-replies to emails advising that filters have been set up to prevent abusive messages from reaching the intended recipient.
-  Use social media monitoring software to track and document ongoing harassment. Be clear about the limitations of this, such as for posts that do not name the researcher and for end-to-end encrypted platforms that cannot be monitored.
-  Discuss whether turning off notifications, locking down social media accounts and blocking accounts might be helpful. This may not always be possible or appropriate, so take care not to oversimplify the decision to engage in online spaces.





Privacy

Provide support for addressing broader privacy concerns, for example:

-  Write a letter of support for the researcher to go on the [unpublished electoral roll](#) so that their home address is not publicly available, and advise the researcher to contact Spark NZ to change their [home listing status](#), if they have a landline.
-  Note that their address may still be publicly available via the company's office, and/or vehicle registry, and email addresses may be publicly available in published academic work.
-  Provide advice and support for researchers who may wish to report abuse to external organisations such as [online hosts](#), [Netsafe](#) and the [Police](#).
-  Provide information about criminal offenses under the [Harmful Digital Communications Act](#) and suggest that the individual access legal support under relevant circumstances.
-  Online harassment can also involve use of the Official Information Act (OIA) process as a form of targeted harassment. Provide expert support for handling OIA requests to protect the privacy and safety of the researcher.

Wellbeing







Support mental health and wellbeing of researchers experiencing harassment:

-  Refer researchers to mental health services, considering the nature of the abuse and the researcher's cultural needs or other demographic factors, where appropriate.
-  Help researchers connect to a broader community of peers—whether those be other researchers who have experienced harassment, or existing networks of researchers with similar backgrounds or expertise.
-  If peer support isn't available, designate an appropriate staff member to check in with the researcher regularly.
-  Provide leave for staff to recover from harassment-related harms.

Communications

Develop strategic internal and external communications plans for potential or actual incidents of targeted harassment.

Plans can be adjusted for different circumstances, ideally with input from the researcher experiencing harassment, and may involve:

-  Inform leaders within the individual's school or department of the situation, including the DVC Māori, DVC Pacific or Rainbow Coordinator, if appropriate.
 -  Communicate internally the institution's commitment to freedom of inquiry and employee safety.
 -  Prepare staff to refer harassing phone calls or other enquiries to the correct department.
 -  Develop media engagement strategies for when instances of online harassment attract wider attention, including public statements reaffirming researchers' expertise, promoting the institution's commitment to academic freedom, and condemning harassment.
 -  Develop plans for responding to fake and misleading information online, including fake advertising and endorsements, deepfakes and misused likenesses of staff.
- TIP:** It may be helpful for institutional leadership to offer personal statements of support and acknowledge that the person's productivity may be impacted due to the emotional strain and time-consuming nature of dealing with the abuse.
-  If the researcher is worried about their reputation among colleagues, help them prepare a brief message for internal circulation explaining their situation and position.






Proactive measures

Protecting researchers from online harm

Visibility

Raise awareness of the availability of support services and key contact points.





Ways of raising awareness include:

-  Train staff who are likely to receive emails and calls about online harassment to respond appropriately to ensure researchers experiencing harassment feel reassured and reach the staff support specialist/ team. A template checklist for any staff receiving reports of abuse is available [here](#).
-  Disseminate information about support services through regular communications and onboarding materials.
-  Include the staff support specialist's contact information in staff email signatures, internal newsletters, and other communications to sustain background awareness.
-  Have the staff support specialist and/or other members of the team, visit and present to different faculties on the support available.
-  Encourage researchers who anticipate future harassment to proactively reach out to support staff.

NOTE: Staff perceptions of whether or not their institutions will 'have their back' can have a significant bearing on whether they engage with media or online spaces, and whether they seek support if this results in harassment.

Outreach

Build relationships with and offer proactive support to at-risk researchers:

-  Identify and build relationships with researchers who have experienced harassment in the past or who are likely to be at risk.
-  Discuss future research, funding announcements, media appearances and public engagement that might attract negative attention.
-  Consider using social media and news monitoring software on an ongoing basis or at key timepoints when researchers may need additional support, with consent.
-  Proactively offer personalised online privacy check ups, feedback, and workshops about digital safety, de-escalation, and other topics for at-risk researchers/ research groups.

NOTE: Consider creating a rubric or other means to identify researchers who may be at risk of harassment due to their ethnicity, gender, sexuality, other demographic factors, public profile, and subject matter expertise. Such risk assessments should be an opt-in service, or carried out with explicit consent of the researcher.

Awareness

Promote digital hygiene and raise awareness about online abuse among all staff.



Create a one-page document outlining how researchers can lock down key settings on social media channels. [PEN America](#) and the [AusSMC](#) have useful resources on digital hygiene best practices. NZ university staff can access this AusSMC resource using their institutional email address.



Create a one-page document outlining how researchers can modify publicly available information on their academic profile, such as their office and classroom locations, contact information, and subject areas. Explain how to request changes to other public-facing pages, directories, and syllabi on institutional websites.



When developing IT systems, carefully consider what information is mandatory to be shown publicly and what can be shown only to logged-in students and staff.



Educate professional staff in relevant roles across different departments about typical patterns, frequency and impacts of online abuse. This will enable staff to build online safety into business processes, corporate systems and advice where possible.



Facilitate an ongoing and open dialogue between IT and staff that respond to incidents of online harassment to ensure both sides are aware of what IT tools and options are in place, how online harassment is evolving, and what documentation or reporting is typically sought in cases of online harassment. This will enable both sides to better support staff and will ensure that good decisions can be made about the procurement and use of IT tools; record-keeping; etc.



Raise awareness among staff about different types of abuse. It is helpful for researchers to understand the broad range of interactions that might be considered harassment, and when to escalate concerns. Even if they feel relatively unaffected by some interactions, reporting concerning incidents can help monitor harassment and protect other staff members from harassment from the same source.

Broader recommendations

Document case studies and feedback from affected researchers



Use case studies and feedback to refine processes and identify measures that were effective under different circumstances.



Collaborate with other institutions to share data and insights and develop best practice.

Recognise the impact of abuse



Establish measures to ensure the impact of abuse - such as reduced productivity or fewer opportunities for public engagement - is duly weighed as a factor in career progress, including in processes for appointment, promotion, and grant applications.



Some impacts may be hard to measure. Researchers may be affected in terms of their willingness to speak as an expert in their field, pursue particular areas of research, or remain in a specific area of research, as a direct result of experiencing harassment or witnessing the harassment of their colleagues.



The volume and impact of abuse tends to be greater for Māori and Pacific researchers, women, sexual and gender minorities. Ensure the equitable distribution of support services and acknowledgement of harms.