External incident flowchart

Tech-based abuse incident occurs

Immediate response

- LIVES: Listen, Inquire needs, Validate, Enhance safety, Support (World Health Organisation, 2014).
- Check safety: If there is an immediate risk, support the employee to call emergency services.
- Preserve evidence: Take screenshots, save messages, preserve digital logs, do not delete records.
- Explain confidentiality: Limit who needs to know, explain mandatory reporting requirements and remind the employee they will not face retaliation for reporting.
- Offer support options: Discuss internal or external support options. For example, local helplines, legal support and counselling services.

Can this be managed with workplace action?

Consider: seriousness, risk, power imbalance, the employee's wishes.

Yes

Direct workplace action

Discuss options with the employee. What would help them?

- Adjust workplace conditions to prevent further harm.
- Support the employee with ongoing check-ins, workload adjustments.

Digital safety action:

- Report then block the alleged perpetrator on the platform by using in-app functions.
- Implement email and IT filters or moderation functions to reduce exposure to potentially harmful content.
- Assist the employee to adjust their privacy and security settings on social media and digital technologies.

See Checklist for further advice.

No

External escalation

Consider engagement outside the workplace:

- Platforms or regulators for takedown requests, removal of content and reporting harms.
- Specialist agencies, such as cybercrime hotlines, non-government organisations or advocate support services.
- Police or legal help for threats, stalking or image-based abuse (only with the employee's informed consent, unless mandatory reporting is required).
- External IT or cybersecurity teams who can assist to trace, filter or mitigate further incidents.

Was the incident resolved and does the employee feel safe?

No

Yes

Outcomes and ongoing actions

- Offer continued support for the employee and remind all parties that retaliation must not be tolerated.
- Monitor for ongoing incidents and develop a rapid response plan.
- Provide a clear and sensitive written outcome to the employee and alleged perpetrator(s), protecting confidentiality.
- Reflect on the root causes of the incident (such as policy gaps, unsafe digital channels).
- Consider updating workplace policies, implementing mandatory tech-based abuse training and improving reporting channels.
- Offer support options: Discuss internal or external support options. For example, local helplines, legal support and counselling services.

APEC Asia-Pacific Economic Cooperation
Australian Government
eSafetyCommissioner