Safer Online Workplaces:
A Toolkit for Empowering Women and Businesses

Policy Partnership on Women and the Economy

October 2026

Asia-Pacific Economic Cooperation

Australian Government

eSafetyCommissioner

APEC Project:
PPWE_04_2024S

Produced by
International Engagement Section, Australia's eSafety Commissioner

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

© 2026 APEC Secretariat

Publication no.
APEC#226-PP-03.2

Asia-Pacific Economic Cooperation

Australian Government

eSafetyCommissioner

Contents

About this toolkit 1

PART I: Understanding tech-based abuse 2

Part Ia – What is tech-based abuse? 2

Common forms of tech-based abuse 4

Editable poster 1: Are you experiencing tech-based abuse in the workplace? 6

Why workplaces must act 7

Part Ib – Tech-based abuse and people: Who does it, who's at risk 8

The perpretrators 9

Who's at risk? 9

Part II: Preventing tech-based abuse at work 13

Building a safe digital culture 13

Editable poster 2: Building your digital safety shield 17

Understanding your risk landscape 18

Getting started: Quick wins for any organisation 18

Checklist for safer use of tech in the workplace 19

Part III: Responding to tech-based abuse at work 22

Examples of immediate actions 23

Other practical measures 23

Editable internal incident flowchart 25

Editable external incident flowchart 26

Dos and don'ts for managers 27

Survivor support and care 27

Appendix 29

Glossary 29

Frameworks 30

References 31

About this toolkit

This toolkit is part of the Australian self-funded Asia-Pacific Economic Cooperation (APEC) project 'Empowering Women and Businesses to Have Safe Online Workplaces', delivered by Australia's eSafety Commissioner with support from the Australian Department of Foreign Affairs and Trade (DFAT). The project is delivered under the APEC Policy Partnership on Women and the Economy (PPWE) and is cosponsored by Chile and Mexico.

The project aims to strengthen the capacity of APEC economies to prevent and respond to technology-related forms of abuse in workplace settings, supporting women's safe and equal participation in the digital economy. It reflects Australia's commitment to advancing online safety, gender equality, and inclusive digital transformation across the Asia–Pacific region.

This toolkit is a practical guide designed for businesses, employers, and human resources (HR) professionals across the 21 APEC member economies. It provides clear steps to prevent, identify, and respond to tech-based abuse in the workplace, recognising that digital safety is a cornerstone of modern workforce wellbeing.

The toolkit:

- raises awareness of tech-based abuse (also known as 'technology-facilitated abuse'), including technology-facilitated gender-based violence (TFGBV) and its impact on women's participation in the workplace
- provides practical tools to prevent and address tech-based abuse, with low-cost, actionable steps
- includes downloadable and editable resources that can be adapted by businesses and organisations in the APEC region to help them address tech-based abuse
- empowers organisations to support women employees' safety online and support their full economic participation.

PART I: Understanding tech-based abuse

PART Ia – What is tech-based abuse?

At a glance: what you need to know

Digital tools have revolutionised work and collaboration, but they can also be misused to harm people.

Tech-based abuse (also known as 'technology-facilitated abuse') occurs when digital tools and platforms - such as email, messaging apps, social media or collaboration tools - are used to bully, harass, threaten or intimidate someone.

This can happen in a workplace context, including between staff in the workplace, while working from home or another remote location, and can involve colleagues, supervisors, customer, clients or suppliers. Abuse can take different forms: it may be fully online, technology-assisted or blended.

Whatever the form, the impact is consistent – tech-based abuse undermines safety, trust and equality at work. Recognising these behaviours early is the first step toward prevention and response.

Digital technologies have transformed how we work, communicate and connect. They enable collaboration across borders and new forms of innovation – but they have also created new ways to cause harm to people.

Tech-based abuse occurs when digital tools and platforms – such as email, messaging services, social media or collaboration platforms – are used to bully, threaten, harass, or harm a person. This can happen in a workplace context, internally or externally.

These same tools that support productivity – video conferencing, messaging channels, social media and project platforms – can be misused to target colleagues or staff.

Tech-based abuse exists on a continuum with offline abuse. Online harassment can escalate into offline stalking or physical harm, and offline abuse can spill into digital spaces.

It can also have other significant emotional impacts, contributing to mental health conditions such as depression and anxiety. Working arrangements can impact an individual's experience of tech-based abuse. For instance, someone who experiences tech-based abuse while working remotely may feel isolated, or someone working in an office setting may feel anxiety about going into the workplace.

Tech-based abuse can also undermine a person's confidence and capability, sometimes causing people to self-censor, exit online spaces or decline promotional opportunities that require them to have public visibility and as a result, an online presence. This chilling effect can in turn limit professional opportunities and economic benefits, particularly for women in the public roles (International Center for Journalists, 2021).

Abuse may be:

- fully online, such as anonymous threats through social media
- technology-assisted, such as recording a private meeting and sharing it without consent
- blended, where online actions escalate into offline harassment, stalking or intimidation.

Myth or Fact #1

Myth:

'If an intimate image has been altered or is fake (such as a 'deepfake'), it doesn't count.'

Fact:

The sharing of intimate images, including images that have been altered or are AI-generated deepfakes, can have devastating impacts on a victim-survivor's wellbeing and reputation. The non-consensual sharing of altered or fake intimate images is still considered as image-based abuse and can cause personal and professional harm.

What can tech-based abuse look like?

This toolkit refers to the 'workplace' as a broad term that includes any location where work is done- an office, onsite and also remote work such as working from home arrangements. The workplace also includes online and offline spaces that could be used both during work hours and outside of work. Tech-based abuse in the workplace can:

- **Occur on a platform or chanel connected to work**: work emails, messaging platforms (such as Microsoft Teams or Slack), social media, online calls (such as Zoom), internal forums, review sites, virtual events or collaboration tools.
- **Involving someone connected to work**: perpetrated by a colleague, manager, contractor, client, customer, supplier, patient, student or member of the public interacting with you due to a person's role. This includes communication to personal devices or accounts.
- **Relating to work identity or activities**: This could be someone being targeted because of their work, or online on media presence related to their work. It could be someone they know or a stranger.

Tech-based abuse can take many forms, but its impact is consistent: it undermines safety, trust and equality at work.

Recognising these behaviours early is the first step toward prevention and response.

Common forms of tech-based abuse

Let's look at the specific behaviours that might be encountered in workplace contexts.

Table 1: Examples of tech-based abuse

Form	What it looks like	Workplace example
Cyberstalking	Unwanted monitoring or contact online – through messages, social media tracking or spyware.	Tracking an employee's location via social media; excessive messaging or surveillance. Note: Managers should be alert if an employee is being harassed across multiple channels, which can indicate intimate-partner violence extending into the workplace.
Digital surveillance or 'spyware' abuse	Breaching privacy by monitoring or hacking someone's devices or communications without consent.	Using workplace technology to track an employee, or a supervisor accessing private messages.
Doxing	The intentional sharing of private or identifying information such as an employee's address or phone number without consent.	Publishing/posting someone's home address or phone number online to invite harassment.
Hate speech and trolling	Abusive, discriminatory or extremist language such as slurs and insults, targeting identity characteristics such as gender, race, disability or sexuality.	Misogynistic, racist, ableist, homophobic or transphobic comments on professional posts; coordinated online harassment targeting women in public-facing leadership positions.
Image-based abuse (including AI-generated images and deepfakes)	Sharing or threatening to share real or digitally-altered intimate, altered or private images or videos without the consent of the person shown.	Altered or stolen images and videos circulated in work chat groups or professional channels.
Impersonation and identity abuse	Hacking an employee's or business accounts or email or creating fake accounts or emails pretending to be someone else to damage their reputation or manipulate others.	A false LinkedIn profile or email account spreading disinformation in an employee's name.
Online sexual harassment	Unwelcome sexual advances, comments, or content shared digitally.	Sexually explicit messages from colleagues or clients or pornography shared through work channels.

Form	What it looks like	Workplace example
Tech-based harassment and bullying	Technology is used to send, post or share content that is seriously harmful to the physical or mental health of a person.	Persistent messages, including emails or chat functions; sharing harmful content after being asked to stop; hostile comments on work-related posts. This may occur one-to-one (for example, a supervisor repeatedly sending harassing messages) or in group spaces where an employee is mocked or excluded.
Threats and intimidation	Direct or implied threats of harm, exposure of private information or retaliation.	Threatening messages sent via email or social media; messages promising to 'ruin someone's reputation.'

An editable version of this A3 poster is available for use in your organisation. Please download at **http://esafety.gov.au/APEC-Safer-Online-Workplaces-Toolkit**

Are you experiencing tech-based abuse in the workplace?

Technology is changing how we work, and that means we need to be prepared for new challenges – including online abuse.

What is tech-based abuse?

Tech-based abuse is when someone uses digital platforms, services or devices to bully, harass, threaten, intimidate or humiliate another person.

It can come from a manager, a coworker or a third party, like a client, customer or community member.

These behaviours can affect anyone, but often disproportionately impact women and marginalised communities including LGBTIQ+ and gender-diverse people.

This behaviour should never be considered part of your job.

What can tech-based abuse in the workplace look like?

Privacy violations

- You're being monitored or stalked through workplace technology like calendars or location-sharing
- Your private information is being shared online without your consent (also known as doxing)
- Your work accounts are being hacked or accessed without permission

Online harassment and bullying

- Abusive comments are being posted on your work or business social media accounts
- Someone is harassing, threatening or intimidating you through emails, messages or online posts
- Someone is making prejudiced online comments based on your gender, sex or sexuality

Impersonation and reputational harm

- Someone has created a fake profile of you to discredit or damage your reputation
- A deepfake or digitally-altered image or video has been made to falsely show you doing or saying something you didn't

Sexual harassment and image-based abuse

- Intimate images or videos of you are being shared without your consent
- You've been sent unsolicited sexual images or asked for nude images – this is sexual harassment

You are not alone.

Tech-based abuse can happen to anyone – even at work.

Asia-Pacific Economic Cooperation

If you believe you are experiencing tech-based abuse, know that you can report it to

[insert reporting pathway and/or support services & logo below]

Why workplaces must act

Violence and harassment at work impacts everyone. Tech-based abuse has real and lasting consequences not only to the individuals that experience it but also their families, businesses, and broader society. These harms mirror those of offline harassment and violence, but can be intensified by the speed, reach and permanence of digital technology.

Table 2: Impact of violence and harassment on the world of work

Scope of impact	Examples of consequences
Individual	**Psychological harm:** stress, fear, anxiety, depression and loss of confidence. **Physical symptoms:** fatigue, headaches, and sleep disturbance linked to chronic stress. **Professional consequences:** withdrawal from online collaboration, reduced productivity, absenteeism, or resignation. **Financial impacts:** loss of income, costs for digital protection or legal advice. For women and gender-diverse employees, these harms can have compounding effects – limiting participation, silencing voices, and constraining career advancement.
Organisational	**Reduced productivity and morale,** as fear or tension spreads within teams. **Increased absenteeism and turnover,** leading to loss of skilled staff. **Damage to trust and workplace culture,** particularly if incidents are mishandled or dismissed. **Legal and reputational risks,** where inadequate prevention or response undermines compliance and public confidence.
Economy and society	**Economic participation:** Lower workforce participation of women and marginalised groups, reduced innovation capacity. **Public systems:** Increased burden on health, justice and social-support services. **Gender equality:** Slower progress toward women's empowerment and inclusive growth. **Democratic integrity:** Targeted online abuse of women in public life undermines free expression and civic participation.

(Source: International Labour Organization, 2020).

PART I: Understanding tech-based abuse

PART Ib – Tech-based abuse and people: Who does it, who's at risk

At a glance: what you need to know

Tech-based abuse can be perpetrated by anyone connected to work and can occur anywhere – onsite, remotely, or outside work hours. Employers have a responsibility to create a safe work environment. Wherever it happens, online abuse is never acceptable and should not be normalised. No employee should be expected to accept online abuse as 'part of the job.'

Tech-based abuse can involve anyone: a coworker, manager, client, customer, supplier or even an anonymous person targeting an employee. It may originate inside the organisation or from outside, such as a disgruntled customer or an abusive partner misusing workplace technology.

Perpetrators

Tech-based abuse can come from anyone related to work – colleagues, senior management, clients or customers.

Men are more likely to be perpetrators of tech-based abuse.

The endorsement of sexist or gender discriminatory attitudes by someone is a good predictor of their being a perpetrator.

Victims or populations at risk

Anyone can be a victim of tech-based abuse, but certain groups are disproportionally affected.

Women, especially young women are more likely to experience unwanted online behaviour – particularly sexual harassment and abuse.

LGBTIQ+ individuals.

Marginalised communities.

Understanding what drives these abusive behaviours can help you design proactive strategies to prevent them.

Anyone can experience tech-based abuse, but certain groups are disproportionately affected, with higher risks or more severe impacts. It can occur onsite, while working remotely, or outside formal working hours. Wherever it happens, online abuse is never acceptable and should never be considered 'part of the job.' Understanding these patterns helps organisations design responses that are inclusive, equitable and sensitive to the realities of different employees.

The perpetrators

Australia's National Research Organisation for Women's Safety (2024) workplace research found:

- One in seven adults (14.9%) reported engaging in technology-facilitated sexual harassment at work.
- Men were more than twice as likely as women to perpetrate such behaviour.
- The strongest predictor of perpetration was the endorsement of sexist or gender-discriminatory attitudes.

Scenario: Client boundary violations

A customer service representative experiences sexually suggestive comments from a regular client during video calls. At first, she tries to redirect the conversation to business, but the comments persist. The client then begins sending LinkedIn messages with similar content outside work hours. When she stops responding, the messages become hostile and accusatory. She worries that reporting the situation might lose an important client and reflect badly on her performance. She continues trying to handle it alone while feeling increasingly uncomfortable and unable to switch off from work.

Individuals who hold sexist or gender discriminatory attitudes were 15 times more likely to engage in workplace technology-facilitated sexual harassment (Australia's National Research Organisation for Women's Safety, 2024). This demonstrates that **tech-based abuse is not caused by technology** itself but is driven by power imbalances, discrimination and cultural norms that tolerate disrespect or inequality.

Who's at risk?

Understanding who is more likely to experience tech-based abuse can help business target their support processes appropriately. If your workplace includes public-facing or high-visibility roles, ensure these employees receive extra guidance and safeguards. If you employ a diverse workforce, recognise that individuals facing multiple forms of discrimination will each have a unique experience, and may require tailored responses when experiencing online or tech-based abuse.

Myth or Fact #2

Myth:

'Women should just be more careful online.'

Fact:

Everyone deserves a safe workplace, including the digital workplace. The responsibility lies with perpetrators and the systems that enable abuse, not with victim-survivors. Everyone deserves safe digital workplaces. Focusing on victims' behaviour rather than perpetrators' actions fundamentally misidentifies the problem and perpetuates cultures that tolerate harassment (UNFPA).

Young women are more likely to experience unwanted online behaviour, particularly sexual harassment and abuse. Plan International's global study (2020) showed that **58% of young women** with Internet access globally have experienced some form of online harassment.

Overall, women experience tech-based abuse more frequently, over longer periods, and with greater psychological harm. Studies show **women are twice** as likely as men to fear for their safety because of online abuse (eSafety Commissioner, 2022). These experiences can affect confidence, wellbeing, and career progression, especially in digital and public-facing roles.

LGBTIQ+ individuals are more likely to face online abuse than others. The Centre for International Governance Innovation's (2023) study across 18 economies found that **75.8% of LGBTIQ+ people** reported experiencing some form of online harm compared to 57.2% of heterosexual people. Similarly, a higher proportion of transgender and gender diverse people reported experiencing any form of online harm (67.8%) than women (59.9%) and men (57%).

Marginalised communities face intersecting discrimination based on factors such as race, ethnicity, disability, gender identity or sexual orientation are more likely to be targeted online. For example, Amnesty International's (2018) research found that **women of colour were 34% more likely** to be mentioned in abusive or harmful content that was hurtful or hostile than white women. In 2026, a survey of women in the United States found that **nearly 1 in 3 (32%) women of colour reported experiencing online abuse**, compared to 24% of white women (National Organization for Women). Respondents identifying as members of racial or ethnic minorities reported **significantly higher rates of online abuse** compared to white respondents (National Organization for Women, 2026).

Women with disabilities are disproportionately impacted by tech-based abuse. Research by eSafety (2021) found that **women with intellectual or cognitive disability may be impacted by a range of harms**, including but not limited to image-based abuse, unsolicited communications, misuse of accounts, abuse and harassment and monitoring via technology. **Barriers to support are complex for women with intellectual or cognitive disability experiencing tech-based abuse**, with many experiencing fear of having devices removed, or of not being believed and feeling trapped because the perpetrator was also her primary carer.

These intersectional risks mean that some employees may need additional support when facing online abuse. This could include tailored training, digital privacy checks, or stronger moderation of public-facing channels, as well as additional considerations for support following an incident.

Family, domestic and sexual violence and tech-based abuse

It is critical that workplaces recognise the risk of employees who may be experiencing tech-based abuse in a family, domestic and sexual violence situation. This can include:

- harassment and abuse online or when using a digital device
- image-based abuse
- stalking and monitoring devices or use of digital devices
- controlling or restricting use of digital devices.

The perpetrator may be a partner, ex-partner, family member or someone living in the home. This may seem like a personal issue that is not relevant to the workplace, but family, domestic and sexual violence can have serious impacts on employees' wellbeing in the workplace. The abuse can even take place on workplace devices or occur during working hours.

Comprehensively addressing tech-based abuse occurring in family, domestic and sexual violence settings is not in the scope of this toolkit. It is, however, essential that employers understand how this may impact their staff and consider opportunities to support them if they are experiencing tech-based abuse in family, domestic and sexual violence situations.

Spotlight: Looking for further guidance on protecting women in leadership from online harm at work?

Free to Lead: Online Harm Toolkit

A practical, free resource designed to help women in public-facing roles, and their employers, stay safe online. Developed by New Zealand's Manatū Wāhine Ministry for Women and Netsafe, the toolkit includes:

- Interactive modules for women and employers
- Information and strategies: how to identify, respond to, and recover from online harm
- Employer guidance: building a culture of online safety and supporting staff

Visit: Free to Lead: Online Harm Toolkit

Women in the Spotlight

eSafety's Women in the Spotlight initiative provides training and resources to raise awareness about gendered online abuse and the ways it can be stopped. This includes **social media self-defence training** to support people who use technology as part of their professional lives to be safer online.

A safe and inclusive digital workplace acknowledges different experiences – and ensures that every employee, regardless of gender, identity, or background, can participate online with confidence and respect.

Workplaces must ensure that digital safety policies and training are inclusive of sexual and gender diversity, and that prevention and response processes consider the diverse needs and experiences of staff to be safe and inclusive for everyone. Recognising what drives perpetration helps workplaces design smarter prevention strategies. When organisations understand that discriminatory attitudes underpin these behaviours, they can target prevention efforts where they matter most:

- Leadership and organisational culture that models respect and accountability.
- Training and awareness raising initiatives that challenge bias and promote empathy.
- Clear, enforced policies that set behavioural standards and consequences.

By addressing the underlying attitudes that enable abuse, workplaces can move from reactive responses to proactive prevention – creating digital workplace environments built on respect, trust and safety for everyone.

Key Takeaways from Part I

- Tech-based abuse is common and can be experienced by anyone, however it disproportionately affects women (particularly young women and those working in public facing roles, culturally and racially marginalised women, women with disability and other marginalised groups such as LGBTIQ+ individuals).
- The drivers of tech-based abuse are cultural, not technological and are rooted in attitudes that tolerate disrespect or inequality.
- Workplace culture matters: environments that normalise harassment and abusive behaviour as 'banter' and blurred boundaries between professional and personal matters create conditions where abuse thrives.
- The costs of tech-based abuse are significant - for individuals (wellbeing and safety), for organisations (productivity and reputation), and for economies (reduced economic participation and lower GDP).
- Addressing tech-based abuse is both a human rights obligation and a business priority for APEC economies striving for inclusive and sustainable economic growth.

PART II: Preventing tech-based abuse at work

At a glance: what you need to know

Preventing tech-based abuse starts with a culture of respect and inclusion. Safe digital workplaces boost trust, productivity, and retention.

Prevention doesn't have to be complex. Key actions include integrating online safety into existing policies and training, establishing clear reporting pathway, modelling respectful digital behaviour, and choosing secure platforms.

Assess your risk landscape and take quick wins like updating policies, reviewing privacy settings, and discussing online safety with teams. Building a safe digital culture is proactive, practical, and essential.

Building a safe digital culture

Prevention measures do not have to be complex or expensive. Many can be achieved by adapting what workplaces already do – integrating online safety into existing codes of conduct, training programs and communication strategies.

Preventing tech-based abuse starts with building a workplace culture where respect and inclusion are the norm. When workplaces prioritise employee safety they can see tangible benefits: higher productivity, lower turnover and stronger employee trust.

Table 3: How to build a safe digital culture

Principle	Practical workplace action	Example
Safe technology management	Choose platforms with privacy controls, blocking features and moderation tools. Limit anonymous posting in internal systems.	Review settings in your collaboration apps (such as Slack or Microsoft Teams) and enable admin controls and privacy defaults.
Leadership and culture	Model respectful online communication. Set the tone from the top. Address inappropriate behaviour promptly.	Include a short 'digital respect' reminder in weekly team meetings or newsletters.
Workplace policy integration	Name tech-based abuse explicitly in conduct, human resources (HR) and health and safety policies. Clarify that digital harassment is workplace harassment.	Add one clear line: 'Harassment using email, messaging, or social media is not tolerated and will be treated as workplace misconduct.'
Training and awareness	Build staff confidence to recognise and respond to online harassment through short, practical refreshers.	Add a discussion to employee induction training: 'What online harassment looks like and how to report it.'
Workplace policy integration	Establish a clear policy and procedure for reporting tech-based abuse, standalone or integrated into existing policies for reporting harm in the workplace. Consider avenues for anonymous reporting.	Familiarise staff with how to report tech-based abuse, emphasising that reports will be confidential. Highlight that retaliation against staff who report will not be tolerated.

Safe technology management

Modern workplaces depend on a variety of digital tools and platforms, such as email, chat, project tools and video conferencing. These systems should incorporate Safety by Design principles and be configured to support employees' privacy.

Key actions:

- Select secure platforms with features that enable moderation, blocking and reporting.
- Protect staff information – avoid publishing personal contact details such as email addresses or photos unless essential.
- Maintain cybersecurity practices – multi-factor authentication, password security, and access controls are essential for both data protection and personal safety.

When selecting or reviewing workplace technology, consider:

- privacy by default
- ability to block or mute users
- clear and accessible reporting pathways
- moderation controls for group environments
- data storage and access security.

What is Safety by Design?

Safety by Design provides guidance to technology companies on how they can reduce online threats by anticipating, detecting and eliminating online harms before they occur.

Developed by Australia's eSafety Commissioner, the initiative provides industry with realistic, actionable, and achievable measures that help minimise online risks and harms and puts users' safety and rights at the centre of the design and development of online products and services.

At the heart of Safety by Design are three principles that provide platforms and services with guidance as they incorporate, assess and enhance user safety:

1. Service provider responsibility
2. User empowerment and autonomy
3. Transparency and accountability

eSafety has also applied Safety by Design principles to technology-facilitated gender-based violence, outlining practical steps that the tech industry can take to prevent and reduce harms impacting women through technology.

Read more about Technology, gendered violence, and Safety by Design

Leadership and culture

Leaders play a critical role in shaping what is considered acceptable behaviour. Good leadership means:

1. Acknowledging the issue: recognise that tech-based abuse is a workplace safety concern, not a personal problem.
2. Modelling respect: ensure digital communications are professional and inclusive.
3. Acting decisively: address tech-based abuse issues promptly and consistently.
4. Embedding accountability: link respectful conduct to performance reviews or leadership competencies.
5. Listening to staff: run periodic surveys or focus groups to identify digital safety risks such as after-hours contact or unmoderated chats.

When leaders model respect online, it signals to staff that everyone has a right to safety and dignity at work.

Workplace policy integration

Policies can translate values into enforceable standards. They should be clear, inclusive, and adapted to the organisation's size and context.

- Define tech-based abuse clearly with examples relevant to the work environment (such as doxing, image-based abuse, impersonation).
- Set clear expectations for digital conduct, including after-hours communication and social media use.
- Implement policies across all communication channels, including internal systems, external platforms and personal devices used for work.
- Link to existing policies – such as the code of conduct, grievance and investigation procedures, IT security and privacy policies, and HR documents.

Awareness and training

Staff are more likely to act respectfully and intervene appropriately when they understand what tech-based abuse looks like and how to respond safely.

- Include short digital safety sessions in onboarding and annual training.
- Share visual reminders such as infographics, posters or intranet messages that show real examples of online harassment.
- Use scenarios and role-play in a safe and trauma-informed environment to help staff identify early warning signs, being alert to potential triggering content for participants who may have experienced harm.
- Train managers in providing survivor-centred approach approaches that protects the safety and dignity of people affected by tech-based abuse, supporting their healing and wellbeing, and prevents further harm from occurring.

Spotlight: Addressing online workplace bullying and harassment in Australia

In collaboration with SafeWork Australia, eSafety designed resources with information and guidance to support workplaces and employees to understand online abuse and how to create a safer online workplace. Grounded in Australia's Work, Health and Safety laws and in line with Australia's 'positive duty' requirements for employers to prevent unlawful or harmful behaviours like sexual harassment in the workplace, the resources offers practical steps to effectively prevent and respond to workplace tech-based abuse.

An editable version of this A3 poster is available for use in your organisation. Please download at **http://esafety.gov.au/APEC-Safer-Online-Workplaces-Toolkit**

Building your digital safety shield

Tools to protect yourself against tech-based abuse at work

If you feel unsafe or you're in immediate danger, call
Abuse can come from anyone – including colleagues, managers and clients.

Speak up

- Remember it's not your fault if you are experiencing abuse, and abuse is never acceptable
- Only if you feel safe to do so – tell the person to stop
- Consider reporting the behaviour to a supervisor or a work safety representative

Secure your devices & accounts

- Change passwords and turn on multi-factor authentication
- Check for unfamiliar apps, settings or devices that may indicate monitoring (for example bluetooth location-sharing devices)
- If you think your work accounts may be compromised, speak to HR immediately

Review social media settings

- Turn off location sharing and location tagging
- Remove, block, or mute unwanted followers – especially if you feel watched or targeted
- Set profiles to private if possible, or limit messaging & commenting functions

Save evidence

- Take screenshots of abusive messages or activity
- Store evidence securely in a USB, the cloud or with a trusted person
- Keep a record of dates, times, platforms, weblinks/URLs and usernames involved

Get support

- Talk to a trusted colleague, supervisor, human resources representative or support service
- Report to law enforcement if you are concerned about your safety

You are not alone.

Tech-based abuse can happen to anyone – even at work.

If you believe you are experiencing tech-based abuse, know that you can report it to

[insert reporting pathway and/or support services & logo below]

Asia-Pacific Economic Cooperation

Understanding your risk landscape

Every business should assess where and how its employees might face digital risks. Incorporating an online risk assessment into existing workplace health and safety reviews can help identify how tech-based abuse might impact your organisation.

Consider the following:

- Conduct a role-based risk assessment: Identify positions most likely to encounter tech-based abuse, such as roles that interact with the public, manage social media accounts, or appear in media.
- Reviewing external factors:
  - Certain industries (such as media, politics, customer service and technology) face heightened risks of online abuse.
  - Stay informed about emerging trends and evolving threats within your sector (such as coordinated or planned attacks on an employee).

Getting started: Quick wins for any organisation

Even small actions can have an immediate effect. Consider the following:

- Adding information about tech-based abuse to your existing harassment or workplace safety policy.
- Reviewing privacy and host controls on collaboration tools like Microsoft Teams or Slack, to ensure that all employees are aware of who has access to staff's online personal information.
- Discussing online safety and respectful communications in your next leadership or team meeting.
- Checking in with staff, particularly those in public-facing roles about their digital safety, including consulting eSafety's social media self-defence resources.
- Displaying and sharing awareness materials and resources about tech-based abuse with staff via email or in shared online spaces.

Key Takeaways from Part II

- Prevention is about designing out harm through changes in workplace technology, culture, and leadership.
- Updating existing policies and staff training can make online safety part of daily operations.
- Completing ongoing online safety risk assessments keeps your workplace responsive as technology evolves.
- A respectful digital culture benefits everyone. It protects people, increases productivity, and protects business reputation.

Checklist for safer use of tech in the workplace

Tech-based abuse refers to the misuse of digital technology to threaten, control, or cause harm to another person. This form of abuse often extends from patterns of harm occurring outside the digital environment.

This checklist provides some tips on how tech-based abuse, including tech-facilitated gender-based violence, can be prevented and addressed in the workplace.

Setting up safer tech

Safe tech management

- Choose software, online platforms and digital tools that prioritise safety, privacy and security. Consider the following:
  - Are privacy, security and legal requirements being met?
  - What data does the service provider collect?
  - Does the service provider use strong encryption?
- Avoid using simple email naming conventions (for example, full names) that make it easy for others to guess email addresses and contact your workers directly.
- Consider using technologies that monitor and filter emails and other workplace communication channels, such as word and phrase filters, to keep them free from abuse. Make sure any monitoring is reasonable and proportionate, and that you consult with workers when making decisions about how to control risks.
- Consider also using filters to limit access to inappropriate websites.
- Avoid having workers use personal phone numbers or social media accounts to communicate with clients or customers.
- Do not post worker information (including full names, videos or photos) without their informed consent.

See also:

- International Labor Organization's 2025 report, 'Revolutionizing health and safety: The role of AI and digitalization at work'.
  - It discusses risk assessment, worker participation and preventive strategies for integrating digital tools safely and effectively in the workplace.
- Australian Cyber Security Centre's 2020 guide, 'Web conferencing security'.
  - It provides guidance for choosing software, online platforms and digital tools.

Understand the risks

If workers are often using WhatsApp, for instance, on their personal devices to communicate with clients and colleagues, implement a WhatsApp code of conduct. This will help ensure that workers are engaging safely on the platform and know where and how to report harms if they occur.

- Understand which platforms and tools are used at work, including websites, social media, email, messaging apps, file sharing services and chat groups.
- Assess whether your existing work platforms and tools meet safety, privacy and security standards. Consider whether the settings can be changed to improve protection. Apply the same assessment to any new tech prior to implementation.
- Check if workers interact with clients, customers or colleagues using their personal devices, or if they need to maintain an online presence as part of their job. If this needs to continue, ask them to do the same safety, privacy and security assessment and adjust their settings to appropriate levels.
- Consider if any staff are more at risk of online abuse, including bullying or sexual harassment.
- Conduct workforce surveys to better identify and understand workplace hazards.

See also:

United Nations Population Fund's (UNFPA) 2023 resource, 'Guidance on the Safe and Ethical Use of Technology'.

Review and revise existing policies and protocols

- Assess existing policies and resources before creating new ones.
- Review existing policies such as safe use of tech in the workplace or training on bullying and harassment to see where you can easily add tech-based abuse.
- Take note of what policies and protocols may be missing, such as a tech-based abuse incident response protocol.
- Make it clear to customers and clients that any form of online harassment or bullying of workers will not be tolerated.
- Moderate public content on your platforms. Consider turning off the comments or sharing features if needed.
- Use platform settings to manage staff privacy and report, block, mute or remove abusive content.

Develop clear reporting pathways

- Seek feedback from all staff, especially women and gender diverse employees, on their needs, wants and challenges, as well as how to control risks of tech-based abuse.
  - Consider anonymous avenues to provide input as well, to ensure staff feel comfortable to provide open and honest feedback.
- Consult with workers to develop easy internal systems for reporting and managing complaints about online harassment, bullying and other abusive behaviours – including confidential, formal, informal or anonymous channels.
- Tailor the procedures to address abuse from customers, clients, the public or other workers.
- Make it clear that blaming a victim for reporting will not be tolerated.
- Encourage supervisors and other staff who are trained to deal with reports of online abuse, to do it promptly and sensitively, ensuring the safety, wellbeing and privacy of everyone involved.

Build workplace culture and skills

- Ensure that employees are aware of appropriate conduct on tech platforms, consequences for inappropriate conduct, how are where to report incidents and support services available both inside and outside the workplace.
  - Consider how codes of conduct will be communicated with workers, such as by providing mandatory awareness training and refresher courses.
- Consider establishing a tech safety and/or gender equality champion, including senior leadership, human resources, ICT staff, to oversee and promote safe use of tech
- Foster an appreciation of diversity. You may like to consider opportunities for diversity and inclusion training.

Reporting online harm

In addition to referring to your workplace policies and procedures, you can suggest workers take the following steps to report serious online abuse.

1. **Collect evidence** – take screenshots and record URLs of what has happened and which platform it occurred on. For more information refer to eSafety's webpage 'Collecting evidence safely' or use Tech Safety Canada's technology-facilitated abuse log.
2. **Report it** – Harmful posts, comments, messages and profiles should be reported to the online platform or service first. You can refer to the The eSafety Guide for guidance on how to report to commonly used platforms, apps and sites. If they don't help, and the abuse is very serious, you may consider reporting to police.
3. **Stop contact** – tighten security settings and prevent content from being shared further.
4. **Get more support** – check eSafety's tips for managing the impacts of adult cyber abuse and image-based abuse.

Note: Remember to obtain consent if you are taking any action on behalf of someone else who may be experiencing online abuse.

More resources

eSafety Commissioner: Workplace bullying

Workplaces Respond: Addressing Violence and Harassment in the World of Work

United Nations Development Programme: Inclusion Toolkit for Organizations and Business

PART III: Responding to tech-based abuse at work

At a glance: what you need to know

A workplace's first response when tech-based abuse occurs is vital in maintaining a culture of trust and safety. A timely, proportionate and survivor-focused response is necessary.

Key actions include responding promptly, assessing the risk, adjusting work expectations, taking practical digital security steps and ensuring support information is provided.

Clear and compassionate responses reassure employees that they are believed and supported. Managers should prioritise safety, dignity, and confidentiality at every step, and ensure that the employees understand their options without feeling pressured.

When tech-based abuse occurs, the first priorities are safety, dignity and support. A timely, proportionate and survivor-centred response prevents escalation, supports recovery and builds trust in workplace systems.

Those who report abuse may feel anxious, exposed or unsure whether they will be believed. They need reassurance that their concerns will be taken seriously, their job is safe, and their information will remain confidential. How you respond sets the tone not only for that person, but for everyone watching how your organisation handles these issues.

Table 4: Guiding principles for supporting employees experiencing tech-based abuse

Principle	What it means	Example
Survivor-centred approach (UN Women, 2011)	Those engaging employees who have experienced tech-based abuse create a supportive environment in which the employees' rights, needs and wishes are prioritised.	Ensure the employee is treated with dignity and respect instead of being exposed to victim-blaming attitudes and can choose the course of action in dealing with incident of tech-based abuse instead of feeling powerless.
Procedurally fair	Ensure transparent, impartial handling for all parties.	Document facts objectively; avoid assumptions or blame.
Confidential and ethical data handling	Share information only with those who need to know and ensure employees privacy is protected.	Store records in a password-protected and access-restricted file.
Timely and consistent	Act quickly, communicate clearly, and apply the same standards across all cases.	Acknowledge the report of tech-based abuse within 24 to 48 hours and provide employee with regular updates.

Examples of immediate actions

- **Respond promptly:** Thank the person for coming forward. Avoid questioning credibility or minimising their experience.
- **Document securely:** Record what occurred, the actions taken, and the date for review. Use neutral, factual language.
- **Assess risk:** Determine whether ongoing digital or physical threats exist. If so, act immediately to protect safety of the employee. This could include:
  - adjusting work locations, duties, shifts or reporting lines
  - resetting passwords or disable compromised accounts
  - rearranging access to workplace systems or premises to avoid contact with the alleged perpetrator, if they are another employee or a client.
- **Protect against retaliation:** State clearly, both verbally and in writing, that retaliation against the employee by the alleged perpetrator and other staff will not be tolerated and may lead to disciplinary action.
- **Provide support information:** Offer details for any available resources such as Employee Assistance Programs (EAP), national online safety, workplace safety, or gender-based-violence hotlines, and internal wellbeing contacts.

Other practical measures

Digital security

- If the employees work accounts are compromised, request the employee to update their passwords.
- Assist the employee to review privacy settings on professional and personal profiles.
- If the incident of tech-based abuse occurred through business-controlled accounts, block or mute harassing content and report through the technology platform.
- Preserve digital evidence of the abuse.

Workplace adjustments

- Temporarily modify duties to reduce online exposure of the employee to online harm.
- Change reporting lines if the perpetrator is a supervisor or manager.
- Offer flexible work hours or location changes for the employee.
- Brief relevant colleagues on confidentiality and boundaries (only with the employees' consent).

Preserving evidence

How to preserve digital evidence:

- Take screenshots showing date, time, username, and content.
- Save messages or emails (do not delete anything).
- Note any witnesses or others who may have seen the content.
- Store everything securely with limited access (password-protected folder, HR file).

Spotlight: Looking for further information on how to preserve and store evidence?

Preserving Digital Evidence Toolkit

A toolkit that helps women, youth, gender-diverse people, and frontline workers preserve digital evidence in circumstances involving technology-facilitated gender-based violence. Developed through Women's Shelters Canada's Tech Safety Canada project, the toolkit provides comprehensive information on preserving and storing incidents of tech-based abuse including a technology-facilitated violence log template that can be downloaded and printed.

Visit: Preserving Digital Evidence Toolkit (Tech Safety Canada)

Privacy reminder: Always comply with data protection laws. Only collect and store what is necessary, with the person's knowledge and consent where possible.

An editable version of this resource is available for use in your organisation.
Please download at **http://esafety.gov.au/APEC-Safer-Online-Workplaces-Toolkit**

Internal 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 and preserve digital logs. Do not delete records.
- Explain confidentiality: Limit who needs to know and explain mandatory reporting requirements. 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, counselling services.

Can this be safely managed inside the organisation?

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

Yes → Direct workplace action

No → External escalation

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.

Investigation:

- Interview the employee, the alleged perpetrator(s), and any witnesses.
- Review available evidence.

Action:

- Consider disciplinary actions.
- Consider implementing permanent digital and `workplace adjustments.
- Provide a clear and written outcome to the employee and alleged

Was the incident resolved and does the employee feel safe?

No → External escalation

Yes → Outcomes and ongoing actions

External escalation

Consider engagement outside the workplace:

- External HR, ombuds, anti-discrimination or labour authority.
- Police or legal help for threats, stalking or image-based abuse (only with the employee's informed consent, unless mandatory reporting is required).
- Platforms or regulators for takedown requests, removal of content and reporting harms.

Action:

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

Outcomes and ongoing actions

- Offer continued support for the employee and remind all parties that retaliation must not be tolerated.
- 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.

Asia-Pacific Economic Cooperation | Australian Government | eSafetyCommissioner

An editable version of this resource is available for use in your organisation.
Please download at **http://esafety.gov.au/APEC-Safer-Online-Workplaces-Toolkit**

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**

No → **External escalation**

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.

Was the incident resolved and does the employee feel safe?

No → **External escalation**

Yes → **Outcomes and ongoing actions**

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.

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.

Asia-Pacific Economic Cooperation | Australian Government | eSafetyCommissioner

Dos and don’ts for managers

Table 5: Actions managers can take in the workplace

Do	Don’t
Respect confidentiality and privacy	Share details with others unless consented to, necessary or required under mandatory reporting obligations
Offer response options and let the employee choose	Impose next steps or demand action
Keep factual, brief notes and follow up regularly	Share documents widely or insecurely
Focus on the employees’ safety and wellbeing	Launch straight into a formal investigation without assessing the risk to the employee
Check in regularly with the employee	Assume one conversation is enough
Respect the employees’ choices	Push the employee to report further or escalate before they are ready

Survivor support and care

A supportive response can prevent long-term harm to employees that experience tech-based abuse and can rebuild their confidence and participation in the workplace.

Table 6: Examples of support

Support type	Practical measures
Psychosocial support	Access to trauma-informed counsellors, peer-support networks or EAP professionals trained in digital abuse.
Technical assistance	Help with device forensics, privacy resets, data removal or social-media escalation.
Legal guidance	Provide information on relevant laws, evidence preservation, and options for police or legal escalation.
Workplace adjustments	Allow temporary remote work, schedule flexibility, reassignment away from the alleged perpetrator, or paid leave for recovery or legal processes.

Key Takeaways from Part III

- A confidential and compassionate response supports recovery and builds trust across the organisation. How you respond shapes whether an employee feels safe, protected, and believed and reduces the risk of future harm.
- How a workplace responds today determines whether others will feel safe to speak up tomorrow. A single supportive response can send a strong signal that the organisation takes tech-based abuse seriously and will act ethically and promptly.
- Early and proportionate action prevents escalation. Quick responses such as assessing risk, protecting digital accounts, and adjusting work arrangements can reduce the risk of further abuse.

Appendix

Glossary

Technology-based abuse (also known as 'tech-based abuse' or 'technology-facilitated abuse') refers to harmful actions carried out online or through digital technology. These include harassment, making threats, stalking and coercive or controlling behaviour. Read more on the eSafety website: About tech-based abuse.

Note: This toolkit recognises that women and gender-diverse people experience these harms more often and more severely, and that addressing these risks is essential for achieving gender equity and safe participation in the digital economy. At the same time, this toolkit acknowledges that tech-based abuse can affect anyone, regardless of their gender, and that using more accessible language helps ensure everyone feels included in prevention and response efforts.

Technology-facilitated gender-based violence (TFGBV) is an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media against a person on the basis of gender. Read more on the United Nations Population Fund website: Technology-facilitated Gender-based Violence: A Growing Threat.

A **survivor-centred approach** creates a supportive environment in which the survivor's rights and wishes are respected, their safety is ensured, and they are treated with dignity and respect. It follows the guiding principles of safety, confidentiality, respect, and non-discrimination. Read more on the United Nations Population Fund in Asia and the Pacific's website: A Survivor-Centred Approach to Monitoring Gender-based Violence Response Programming.

Safety by Design is a prevention-focused approach developed by Australia's eSafety Commissioner that builds safety into technology and systems from the start. Originally developed for tech companies, Safety by Design means building safety considerations into technologies from the outset. The aim is to shift the burden of safety away from individual users to the tools and systems we use. Read more on the eSafety website: Safety by Design.

World of Work includes any physical, digital, or hybrid environment where work occurs, is organised, or arises. This includes:

i) A physical workplace, including public and private spaces,
ii) A place where a worker is paid, takes a rest or a meal, or uses sanitary, washing or changing facilities,
iii) Work-related trips, travel, training, events, or social activities,
iv) Work-related communications, including those enabled by information and communication technologies,
v) In employer-provided accommodation, and
vi) Commuting to and from work

See: **ILO Convention No.190, Article 3** Convention C190 - Violence and Harassment Convention, 2019 (No. 190)

Note: Throughout this toolkit, 'workplace' is used a plain language way of referring to what the International Labor Organization defines as the broader 'world of work'. It also includes situations that arise out of or in the course of work. Employers should recognise that abuse can also extend beyond formal work environments or outside working hours – occurring in homes, on social media or through private messages.

Frameworks

ILO Convention 190 (Violence and Harassment): International Labour Organization convention recognising the right to a world of work free from violence and harassment, including gender-based violence. It recognises that violence can occur in the workplace, through work-related communications (including technology), and that employers and governments should take measures to prevent and address it. See: Convention C190 – Violence and Harassment Convention, 2019 (No. 190)

ISO 45003 – Managing Psychological Health and Safety in the Workplace: In 2021, the International Organization for Standardization issued ISO 45003, guidelines for managing psychological health and safety at work. This standard guides employers to identify and mitigate psychosocial hazards – which include workplace bullying and harassment, whether offline or online – as part of their occupational health and safety management. See: ISO 45003:2021 – Psychological health and safety at work.

References

Amnesty International. (2018). *Crowdsourced Twitter study reveals shocking scale of online abuse against women*. https://www.amnesty.org/en/latest/press-release/2018/12/crowdsourced-twitter-study-reveals-shocking-scale-of-online-abuse-against-women/

Australian National Research Organisation for Women's Safety. (2024). 'Workplace technology-facilitated sexual harassment: Perpetration, responses and prevention'.

Centre for International Governance Innovation. (2023). 'Supporting Safer Digital Spaces'.

eSafety Commissioner. (2021). 'Technology-facilitated abuse of women with intellectual or cognitive disability'

eSafety Commissioner. (2022). 'Women in the Spotlight: How online abuse impacts women in their working lives'.

eSafety Commissioner. (2025). *Online risks for women.* https://www.esafety.gov.au/women/online-risks-for-women

eSafety Commissioner. (2024). *Technology, gendered violence and Safety by Design: An industry guide*. https://www.esafety.gov.au/industry/safety-by-design/industry-guides#technology-gendered-violence-and-safety-by-design

eSafety Commissioner and Safe Work Australia. (2025). 'Checklist to create a safer online workplace'.

eSafety Commissioner and Safe Work Australia. (2025). *Online abuse in the workplace – employer information*. https://www.esafety.gov.au/key-topics/workplace-bullying-and-harassment/employers

eSafety Commissioner and Safe Work Australia. (2025). *Online abuse in the workplace – worker information*. https://www.esafety.gov.au/key-topics/workplace-bullying-and-harassment/workers

eSafety Commissioner. (2025). *Online risks for women.* https://www.esafety.gov.au/women/online-risks-for-women

International Center for Journalists. (2021). 'The Chilling: A Global Study On Online Violence Against Women Journalists'.

International Labour Organization. (2020). 'Safe and healthy working environments free from violence and harassment'.

International Labour Organization. (2019). *Violence and Harassment Convention, 2019 (No. 190)*. https://normlex.ilo.org/dyn/nrmlx_en/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:3999810

Monash University. (2022). *Half of all Australians will be victims of technology-facilitated abuse, new research finds*. https://www.monash.edu/news/articles/half-of-all-australians-will-be-victims-of-technology-facilitated-abuse,-new-research-finds

National Organization for Women and Incogni. (2026). 'Online Abuse Against American Women is Escalating'.

Plan International. (2020). *State of the World's Girls 2020: Free to Be Online?*. https://plan-international.org/publications/free-to-be-online/

The Economist Intelligence Unit. (2021). *Measuring the prevalence of online violence against women*. https://onlineviolencewomen.eiu.com/

UNESCO. (2021). *The Chilling: Global trends in online violence against women journalists.* https://unesdoc.unesco.org/ark:/48223/pf0000377223

United Nations Population Fund. (2014). 'Strengthening Health System Responses to Gender based Violence in Eastern Europe and Central Asia'.

United Nations Population Fund. (n.d.). *Technology-facilitated Gender-based Violence: A Growing Threat*. https://www.unfpa.org/TFGBV

United Nations Women. (2016). *The economic costs of violence against women*. https://www.unwomen.org/en/news/stories/2016/9/speech-by-lakshmi-puri-on-economic-costs-of-violence-against-women

United Nations Women (2022). *Learning from practice: Survivor-centred, multisectoral service provision as part of Prevention of Violence against Women and Girls*. https://untf.unwomen.org/en/digital-library/publications/2022/05/learning-from-practice-survivor-centred-multisectoral-service-provision-as-part-of-prevention-of-violence-against-women-and-girls

United Nations Women. (2025). *FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women and girls*. https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women

APEC Project:
PPWE_04_2024S

Produced by
International Engagement Section, Australia's eSafety Commissioner

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

© 2026 APEC Secretariat

Publication no.
APEC#226-PP-03.2

Asia-Pacific Economic Cooperation

Australian Government

eSafetyCommissioner