Australian Government | acma Australian Communications and Media Authority

Domestic, Family and Sexual Violence Standard

Industry guidance

JANUARY 2026 – VERSION 2

This guide applies to carriage service providers in their dealings with consumers and carriers in relation to their supply of carriage services to carriage service providers.

This guide will be reviewed and updated as feedback is received, or new information becomes available. Updated versions will be published, and telcos will be notified when changes occur to ensure they have the latest guidance.

Canberra
Level 3
40 Cameron Avenue
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 32
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
F +61 2 9334 7799

Contents

Overview

1. Purpose of this guide

Carriers and carriage service providers (telcos) are required to comply with the Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025 (the Standard), which sets out mandatory requirements for responding to, and supporting, consumers who are, or may be, affected by domestic, family and sexual violence.

The Standard was developed to give effect to the objectives outlined in section 7 of the Telecommunications (Domestic, Family and Sexual Violence Consumer Protections Industry Standard) Direction 2024.

The ACMA recognises the critical role the telecommunications sector plays in protecting consumers affected by domestic, family and sexual violence. The Standard reflects a commitment to safeguarding victim-survivors' rights to privacy, safety and continued access to communications services.

The purpose of this guide is to assist industry in understanding and implementing the requirements in the Standard in a way that prioritises safety, privacy and security of affected consumers. It also clarifies how the Standard interacts with other regulatory instruments and obligations. Where there is inconsistency, the Standard takes precedence over industry codes and guidelines.

While this guide is intended to signal the ACMA's expectations, it is guidance only. This guide does not constitute or replace legal advice on obligations under the Standard. Telcos should seek independent legal or compliance advice to ensure compliance with all applicable laws and obligations.

This guide uses initialisms (for example, DFSV and DFV) when referring to terminology as written in the Standard. This is to provide clear and easy reference guidance for telcos.

We **do not advise** that telcos use these initialisms in their public-facing content, or with interactions with their customers.

Telcos should refer to the advice they receive as part of their consultation with experts on how to refer to domestic, family and sexual violence in public-facing communications and with customers.

2. Using this guidance

This Domestic, Family and Sexual Violence Standard industry guidance gives practical support (for example, information about the ACMA's approach to a particular issue or describing the steps of a process).

It includes practical examples to assist telcos in providing support, developing policies, procedures and training that prioritise security and privacy for affected persons.

This guidance must be read in conjunction with:

(a) legislation and regulation (mandatory), including the current versions of:

i. the Standard and its Explanatory Statement[1]

ii. the *Telecommunications Act 1997*

iii. the *Telecommunications (Consumer Protection and Service Standards) Act 1999*

iv. the *Privacy Act 1988*

v. the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022

vi. the Telecommunications (Financial Hardship) Industry Standard 2024

vii. the Telecommunications (Consumer Complaints Handling) Industry Standard 2018

viii. the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017.

ix. the Telecommunications Numbering Plan 2025.

(b) industry codes:

i. C556 Number Management – Use of Numbers by Customers Industry Code

ii. C628 Telecommunications Consumer Protections (TCP) Industry Code

iii. C525 Handling of Life Threatening and Unwelcome Communications Industry Code.

Information in this guidance is general and does not limit or prevent the ACMA from taking enforcement action.

3. Why the Standard was needed

Domestic, family and sexual violence causes profound harm across Australian society, impacting individuals' safety and wellbeing. Victim-survivors often face complex challenges including coercive control, economic abuse and technology-facilitated harassment.

Telecommunications services play a critical role in helping affected persons to stay connected to support networks, access emergency services and maintain privacy and autonomy. However, these same services can also be misused by perpetrators to monitor, isolate or control. How a telco provides services to a victim-survivor can assist them if done well, or exacerbate the risks and harms caused by domestic, family and sexual violence if not.

Recognising the vital role of telcos in safeguarding vulnerable consumers, the Australian Government directed the ACMA to develop the Standard to establish enforceable protections and ensure consistent, trauma-informed support across the sector.

[1] Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025 accessed on the Federal Register of Legislation

4. The role of industry under the Standard

Each telco is:

- responsible for ensuring compliance with the Standard, including obtaining legal advice where needed, to ensure their measures and implementation are consistent with the requirements under the Standard
- required to support affected persons to remain connected to a telecommunications service
- required to develop and implement safe, inclusive and effective policies and procedures, which should be informed by consultation with appropriate experts and people with lived experience.

Telcos are not responsible for crisis support for people impacted by domestic, family and sexual violence. This support should be provided by domestic, family and sexual violence specialist services and other appropriately trained experts.

5. What is 'domestic, family and sexual violence'?

In this guide 'domestic and family violence' is used as an umbrella term to incorporate the definitions of both domestic and family violence and sexual violence.

Domestic and family violence refers to behaviours of an individual that are designed to create a dependency or to isolate, monitor, dominate or control another individual. These behaviours can be physical or non-physical and can occur in a variety of personal relationships, including between intimate partners, parents and children, family groups, kinship connections and in carer and guardianship arrangements.

'Sexual violence' is sexual behaviour that occurs where consent is not freely given or obtained, is withdrawn or the individual is unable to consent due to their age or other factors and can be physical or non-physical.

These provisions are defined at section 5 of the Standard.

6. What is 'coercive control'?

Coercive control is a term used in the definition of 'domestic and family violence' in section 5 of the Standard.

Coercive control is a repeated pattern of behaviour used by an individual that has the effect of creating and maintaining control over another individual by exerting power and dominance in everyday life to deny freedom and autonomy through fear, control, pressure or manipulation. Coercive control may be more subtle and less obvious than other forms of domestic and family violence, which is why it is important that industry policies, procedures and training address this behaviour.

For example, it may present as, but is not limited to, a perpetrator:

- forcing the affected person to add the perpetrator as an authorised representative on the affected person's account
- restricting the affected person's access to telecommunications services. This may be through physical action (for example, removing a device, disconnecting an internet connection) or non-physical means (for example, screen time limits or restrictions)
- using telecommunications services to monitor the affected person's location, movement, calls, communication, internet usage or other actions.

7. What is a 'consumer'?

The term 'consumer' is an important part of several definitions in the Standard.

A consumer can be:

- an individual using a telco service for personal use (not for resale)
- a not-for-profit organisation using the service for its own operations (not for resale)
- a small business that:
  - uses the service for its own purposes (not for resale)
  - is not given a reasonable opportunity to negotiate the contract terms
  - spends no more than $40,000 a year with the telco.

An authorised representative is also considered a consumer.

8. When the rules in the Standard commence

The requirements in the Standard are being implemented in 2 phases:

- **Phase 1** – some requirements commenced on 1 July 2025 and are currently in effect.
- **Phase 2** – remaining requirements will commence progressively in 2026 depending on the size of the telco.

This guidance outlines the full set of responsibilities under the Standard, including those already in effect and those commencing in 2026.

9. Phase 1: from 1 July 2025

From 1 July 2025 **all telcos** must:

- if a customer's service has been disconnected, suspended or restricted, reverse the action without delay, when the customer makes an urgent request because of a domestic and family violence-related safety risk. If a reversal isn't practical, the telco must offer the customer an equivalent telco service (subsections 13(3)– (5))
- not require an affected person to contact or engage with an alleged perpetrator, or with their representative. This protects individuals from further trauma, intimidation or safety risks that could arise from such interactions (subsection 15(1))
- publish website information about what domestic and family violence support it offers and how affected persons can access it. If a telco does not currently offer support, it must provide information about organisations the customer can contact to get support (section 16)
- commence developing domestic and family violence policy and procedures (section 19)

- commence domestic and family violence training for all of its staff, including specialised training for staff who deal directly with general enquiries from consumers and staff who deal with domestic and family violence issues for the telco. For example, areas in sales, credit collections, financial hardship, fraud, privacy and complaints (sections 21 and 22)
- consult with domestic and family violence experts and people with lived experience of domestic and family violence, when developing its policies, procedures and training (section 32).

10. Phase 2: From 1 January 2026 or 1 April 2026

Depending on the number of services in operation, the remaining requirements under the standard (the deferred rules) commence on:

- **1 January 2026:** Large telcos (30,000 or more services in operation on 1 July 2025)
- **1 April 2026**: Small telcos[2] (less than 30,000 services in operation on 1 July 2025).

The deferred rules are set out in the following sections:

- Section 7 – Requirement where a consumer has experienced sexual violence outside a domestic and family violence situation
- Section 8 – Requirement to advise affected persons of available support
- Section 9 – Application of sections 10 and 11
- Section 10 – Requirement to agree on a preferred communication method
- Section 11 – Requirement to discuss support options
- Section 12 – Minimum requirements for support
- Subsections 13(1), (2) and (6) – Providing support to affected persons
- Section 14 – A provider must not require evidence
- Subsections 15(2)-(5) – Communications with affected persons
- Section 17 – Requirement to publish a DFV statement
- Section 18 – Requirements regarding access to DFV support services
- Section 20 – Minimum requirements for DFV policies and procedures
- Section 23 – Requirement to review policy and procedures
- Section 24 – Requirement to monitor personnel
- Section 25 – Requirements relating to the security and privacy of an affected person
- Section 26 – Requirement on carriers to provide assistance
- Section 27 – Security of personal and sensitive information
- Section 28 – Privacy
- Section 29 – Where privacy is breached
- Section 30 – Requirements to keep records
- Section 31 – Record retention

[2] Section 4 (2)

11. What telcos must be doing in 2026

In addition to ensuring compliance with the requirements under the Standard from 1 July 2025, **all telcos** must meet all the requirements set out in the deferred rules, from either 1 January 2026 or 1 April 2026, as relevant, including to:

- support a consumer that has experienced non-domestic sexual violence in the same way as a domestic and family violence consumer when providing or offering telecommunications support (section 7)

  > Non-domestic sexual violence means sexual violence that has occurred outside a domestic and family violence situation – for example, with acquaintances or strangers.

- provide affected persons with clear, accessible information about available domestic and family violence support and how to access it, including (sections 8–12):
  - advising and agreeing on a preferred communication method (section 10)
  - the option to set up a new account that is not linked to the perpetrator (paragraph 12(a))
  - the option to add account protections such as a PIN or verification code (paragraph 12(b))
- not require an affected person to disclose evidence which demonstrates the person is an affected person, unless that evidence is required by law or is needed to protect the interests of an affected person (subsection 14(2))
- not require an affected person to disclose the circumstances of the abuse in order to receive support (subsection 15(2))
- establish requirements for warm transfers (defined in section 5) to ensure affected persons do not to have to repeatedly explain their circumstances, which may cause further distress (subsections 15(3)-(4))
- change the billing delivery method or billing address if the affected person makes a request (subsection 15(5))
- publish a DFV statement on its website and provide multiple contact channels to access direct support. For example, via a specialist support phone number, a dedicated web form, online written chat, in person at a retail store or by email (section 17 & subsection 18(1))
- only contact an affected person at the time requested using the method requested if the affected person asks a telco to initiate contact or to call them at a later time (subsection 18(3))
- review policies and procedures and develop an internal monitoring program to assess its staff compliance with its DFV policies and procedures (sections 23-24)
- meet security and privacy requirements, including hiding the following support telephone numbers on any bill, record or other material (subsection 25(3)):
  - 1800RESPECT: 1800 737 732
  - 1800ElderHelp: 1800 353 374
  - Full Stop: 1800 385 578
  - National Debt Helpline: 1800 007 007
  - National Disability Abuse and Neglect Hotline: 1800 880 052
  - Rainbow Sexual, Domestic and Family Violence Helpline: 1800 497 212.

12. Why the Standard applies to businesses and not-for-profit (NFP) consumers

The Standard applies to a broad range of 'consumers', including small businesses and NFPs as defined in section 5 of the Standard. This means that telcos must apply the protections under the Standard to eligible small business and NFP consumers – not just individuals.

We understand that many victim-survivors operate as sole traders or run small businesses, and perpetrators often target those business services along with their personal accounts. For example, a perpetrator may misuse the business's telecommunications services – such as diverting calls, locking accounts, cancelling a service – to control an affected person and cause them harm. Even if the service is registered to a business or organisation, telcos still have a responsibility to recognise the risk and provide appropriate support.

To ensure consistent coverage, the ACMA adopted the definition of 'consumer' from the Telecommunications (Financial Hardship) Industry Standard 2024 (the Financial Hardship Standard), which includes small business and NFPs in similar contexts.

Frequently asked questions

The parts references in the following sections relate to the parts of the Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025.

Part 2 – Sexual violence outside a domestic and family violence situation

What is sexual violence outside a domestic and family violence situation and who can it involve (section 7)?

Sexual violence means sexual behaviour where consent is not freely given or obtained, is withdrawn or the individual is unable to consent due to their age or other factors. It may be physical or non-physical and occurs when an individual is forced, coerced or manipulated into sexual activity.

Sexual violence outside a domestic and family violence context refers to incidents that are not connected to domestic and family violence relationships. This can involve harm caused by individuals such as strangers, acquaintances, colleagues or others outside the family or caregiver environment.

For the purpose of this Standard, this does not include sexual violence perpetrated by intimate partners, parents, children, extended family members, guardians or carers, which fall inside a domestic and family violence situation.

What must a telco do if a consumer discloses that they have experienced sexual violence outside a domestic and family violence situation?

If a consumer advises a telco that they have experienced sexual violence that is not related to domestic and family violence, the telco must provide support in line with certain key protections, including:

- subsection 8(2) – to advise of the support offered under its DFV policy
- section 10 – to agree on preferred communication method
- section 13 – to provide ongoing support and reverse service limiting actions
- section 14 – to not require evidence, unless legally necessary
- subsections 15(2)-(4) – to not require disclosure of the circumstances of the abuse and to offer a warm transfer.

Example

Alex contacts their telco to discuss a recent service disconnection. During the call, they disclose that they have experienced sexual violence from a stranger. They explain that they urgently need their mobile service reconnected as the perpetrator has threatened to return.

Telco obligations

Under the Standard, Alex must be treated as an affected person, even though the violence occurred outside a domestic and family violence context. The telco must:

- confirm it is safe to communicate with Alex and if so advise them of the telco's DFV support
- offer and agree on a preferred communication method
- not request any evidence of the sexual violence, respecting Alex's privacy and trauma
- offer a warm transfer to relevant staff, including to specialised support or reconnection teams
- urgently reverse the service disconnection due to safety.

Response/outcome

Alex's service is restored the same day. They receive follow-up support via their preferred communication method and are referred to external support services listed in the telco's DFV statement.

Part 3 – Providing support

What support information do I need to provide to an affected person (section 8)?

Telcos must first check with the affected person whether it's safe for them to communicate with the telco.

Once a telco has confirmation that it's safe to communicate, the telco must provide to the affected person specific information set out in the Standard. This includes:

- that it can assist the customer in accordance with its DFV policy
- provide information about its specialised domestic and family violence team (if it has one) and that they can receive a 'warm transfer'
- referring the customer to support organisations listed in the DFV statement on its website.

A 'warm transfer' means when a telco staff member (or system) passes an affected person's query to another staff member but first explains the situation to that staff member, so the customer doesn't have to repeat their story. This can happen over the phone or through online chat.

Do telcos need to inform affected persons about available communication methods and how they prefer to be contacted (section 10)?

Yes. Under subsection 10(1) telcos must clearly outline the available communication methods (for example, telephone, email, SMS) and ask the affected person which option they prefer. They must also check if the customer has a preferred time of day to be contacted.

If the affected person asks for an **agreed communication method**, telcos must only use that method when contacting the customer. However, paragraph 10(3)(b) allows telcos to use a different communication method if the affected person initiates contact through that method. In such cases, the telco should use appropriate verification methods to confirm they are speaking with the affected person or their authorised representative. This may include enacting measures to protect the privacy and security of an affected person's information such as a two-step authentication or placing a Personal Identification Number (PIN) on the account for access. The telco should also confirm whether the person wishes to update their preferred contact method or if it's a one-off change.

Example

Jamie has an agreement with their telco for contact to be via their mother's phone number, which is not the account phone number, between 10 am and 11 am on Wednesdays. Jamie contacts their telco on a Thursday afternoon requesting an urgent call back to a different phone number.

Telco action

The telco may use that different phone number to return Jamie's call. The telco checks that they are speaking with Jamie by asking Jamie to provide the PIN that has been added to the account to protect it from access by third parties including the perpetrator.[3]

The telco also asks Jamie whether they would like to change their agreed communication method, or whether this is a one-off change to communication.

Example

Rose's agreed method of communication is to a Hotmail account she accesses from a library terminal while living with the perpetrator. Rose contacts her telco and advises that she would like all future communications to be sent via her financial counsellor and provides the telco with a contact number.

Telco action

The telco should use the number of the financial counsellor to contact Rose. The telco should have processes and procedures in place to update Rose's information, including information for her to enact the relevant authorisations.

[3] For the purposes of the examples in this guide it is taken that in each case the telco has taken the appropriate steps to verify they are speaking to the affected person or their authorised representative.

What should a telco do if a customer advises that their current communication method is no longer safe or has been compromised?

The telco must assist the customer in changing the communication method and offer to set up a new account that is not linked to the perpetrator. The telco must also offer safety and security protections such as a PIN or password on an account or sending a verification code to a 'safe' number or email address.

Example

Emily contacts her telco's support team and discloses that she is experiencing domestic violence. She explains that her account is protected by Multi-Factor Authentication (MFA,) but the verification code is currently sent to her mobile number – which her perpetrator has access to. She's worried that any attempt to change her account settings or receive support will be intercepted and requests that all future communications are via her provided email address.

Telco action

The telco should confirm with Emily whether it is safe to communicate and provide the required information, including an offer for a warm transfer to their domestic and family violence support specialist (which Emily accepts). The specialist discusses Emily's concerns and offers support options, including:

- changing the MFA destination to a secure email address that only Emily can access
- adding a secondary verification method using a secure app or token
- placing a PIN on the account to prevent unauthorised access via customer service channels.

The telco offers to set up a new account not linked to the perpetrator and ensures that all future communications follow Emily's preferred method (email only).

What happens if there is a potential conflict with the communication methods required by different instruments?

There may be situations where telcos are required to use a specified method to communicate with a consumer that is not compatible with the 'agreed communication method'. The Standard has an exception at subsection 10(3) for this situation. However, it is important that a telco's actions do not contravene its obligations to secure an affected person's information from disclosure to a perpetrator under subsection 27(2).

For this reason, where a telco has an obligation to use a specific communication method, for example the requirement to advise of an outcome in writing at paragraph 13(l) of the Telecommunications (Consumer Complaints Handling) Industry Standard 2018 (the Complaints Standard), telcos should first discuss this with the affected person prior to sending any notifications or communications that require it to use a method other than the 'agreed communication method'.

It is important to recognise that for complaints, communications should be with the consumer who made the complaint, irrespective of whether they are the account holder or end user.

What does reverse the service limiting action 'urgently' mean (paragraph 13(3)(b))?

Telcos must reverse any service limitation – such as a disconnection, suspension or restriction – when an affected person first contacts the telco due to a domestic and family violence related safety risk. 'Urgently' means that a reversal must be actioned **immediately** with service restoration treated as a priority to support the safety and wellbeing of the affected person.

Urgent reversal of service limitations includes:

- **Prompt restoration of services:** disconnections, suspensions or restrictions (such as blocked calls, suspended mobile data) must be reversed without delay.
- **No engagement with perpetrator:** the affected person must not be required to engage with the perpetrator to resolve account issues or outstanding debts before service reconnection is actioned.

Note: Rules for disconnection or suspension of phone numbers are outlined in Industry Code C566 Number Management – Use of Numbers by Customers (the UON Code), including specific provisions for customers affected by domestic and family violence. When a phone number is disconnected, the number must go into quarantine for 6 to 12 months. If a telco identifies, or is advised of, a service that was incorrectly disconnected and it holds the number in quarantine, the telco must recover the number from quarantine and re-issue it to the customer in one business day (clause 7.1.3).

Note: While the Standard does not prescribe a specific timeframe for reversals due to a 'domestic and family violence related safety risk', **one business day,** as for the UON Code, is likely to be considered a reasonable and appropriate benchmark for urgent reconnection in these circumstances (paragraph 13(3)(b)).

What is a domestic and family violence related safety risk?

A domestic and family violence related safety risk (subsection 13(3)) is where there is a likely and serious risk of harm to the affected person or their children, and their telecommunications service plays a material role in increasing or reducing the risk. Examples include, but are not limited to, when an affected person:

- would not be able to call emergency services (like 000) or other services that are part of their safety plan for an emergency
- has lost access to services used for security such as multi-factor authentication, password verification or recovery, which are necessary to manage imminent safety risks or to access internet connected safety devices (for example, security cameras).

The circumstances of the particular matter, as conveyed by the affected person, need to be carefully considered in assessing the risk. For example, restriction on the speed of a data service may not have the same risk assessment as disconnection of the person's only phone service.

What is an equivalent telecommunications service (subsection 13(4))?

An equivalent telecommunications service is one that:

- provides the same type of service – such as mobile, internet or a bundled service
- is the same or lower cost – not more expensive than the original service
- is the same quality – similar speed, data, coverage and features.

This ensures an affected person can stay connected without losing access or paying more.

For example, if the customer has a mobile and internet service used to support security cameras, the telco must offer a replacement service with equivalent data services that meets the customer's needs and at the same or lower cost.

Does the loss of a prepaid mobile service where that service is not recharged at the end of a prepaid period count as a 'service limiting action' under subsection 13(3)?

No. A service limiting action is when a telco has restricted, suspended or disconnected a customer's service. A customer who has failed to recharge their prepaid service causing an interruption to the provision of their service will be able to have their service recommence after recharge. Consequently, we do not consider that the interruption to service caused by a customer's failure to recharge constitutes a service limiting action by a telco under section 13.

However, in circumstances where an affected person self-identifies a domestic and family violence situation and re-charging would not result in recommencement (for example the service had been terminated by the telco), the service would be considered disconnected. In that case, reconnection obligations under subsections 13(3) or 13(4) would apply.

If a prepaid service has not been recharged and the consumer requests reconnection due to a domestic and family violence risk, rules under Part 3 (sections 14–18) of the Financial Hardship Standard may also apply.

Can telcos provide a replacement service, such as a prepaid mobile service, to consumers affected by domestic and family violence without ID checks?

Yes, but only under specific conditions set out in section 3.2 of the Telecommunications (Service Provider-Identity Checks for Prepaid Mobile Carriage Services) Determination 2017 (Prepaid Determination). Telcos can supply a prepaid mobile service without conducting an ID check if the:

- service and handset are provided through a family violence assistance organisation (for example, a shelter);
- organisation reasonably believes the person is affected by family violence and collects their name and address – unless it's not safe or impractical; and
- service is limited to 30 days, unless the ACMA has approved a longer period.

Can telcos apply for longer activation periods for prepaid services?

Yes. Telcos can apply to the ACMA to extend the standard 30-day activation period to enable customers affected by domestic and family violence more time to obtain the necessary ID documents. An application must be made in writing and explain the reason for the extension, the duration of the extension and the service or services it applies to. The ACMA assesses requests on a case-by-case basis. While there is no fixed timeframe, exemptions are usually processed promptly when applications are complete and urgent.

Some telcos have applied for and been granted exemptions that enable them to supply prepaid mobile services to customers affected by family violence (as a specified class) for up to 90 days (instead of 30 days) before needing to meet the ID verification rules. These applications may take longer to be considered, but they too are actioned promptly by the ACMA. Please contact national.interests@acma.gov.au for further information.

What if a telco wants to offer alternative ID options for prepaid services?

Telcos may offer alternative verification options for prepaid services, provided they receive approval from the ACMA. This is because telcos must comply with the identity verification requirements set out in Part 4 of the Prepaid Determination, unless exempt under Part 3 of the Determination or operating under an ACMA approved compliance plan under Part 5. A compliance plan allows telcos to propose alternative processes for collecting and verifying customer IDs. These processes must demonstrate how they meet the objectives of the Prepaid Determination.

Telcos are encouraged to explore whether alternative ID verification methods could better support individuals who face challenges with traditional forms of identification. Where appropriate, these alternatives can be submitted through individual or joint compliance plan applications. All plans must be approved by the ACMA to ensure regulatory compliance. Telcos are also encouraged to contact the ACMA to discuss potential compliance plan proposals before submitting an application.

Note: The ACMA will soon amend the Part 4 rules in the Prepaid Determination to formally recognise Digital ID as a valid method of identity verification.

In what limited circumstances can a telco require evidence that a customer is an affected person (section 14)?

People affected by domestic and family violence often face significant emotional and practical challenges when seeking support. Requiring them to prove their circumstances can cause distress and deter them from seeking help. For this reason, telcos should avoid requesting unnecessary evidence. However, evidence may be required in limited circumstances, including:

- **Legal obligations** – where a telco is subject to a court order or law enforcement request or where compliance with privacy, fraud or security laws necessitates evidence.
- **Protecting interests of an affected person** – where there is serious risk to a person's safety (whether or not that risk relates to the affected person seeking help or another person) or where evidence is needed to prevent misuse of services.

Guiding principles:

- The starting point should be to trust the consumer's statement.
- Each situation must be assessed carefully with the primary focus on the consumer's safety.
- The term '*protect the interests of an affected person*' refers specifically to safeguarding the safety, privacy and continued access to services of that person.
- The affected person may not always be the individual making the request – telcos must remain alert to the potential misuse of domestic and family violence protections. If there are reasonable concerns that the person requesting support is not the affected individual, telcos can request evidence to alleviate those concerns.
- In complex cases where you may have questions or concerns, seek guidance from domestic and family violence experts.

Before requesting evidence, telcos should check internal records to see whether existing information supports a customer's claim and ensure any request for evidence is well-justified.

This provision is intended for exceptional circumstances and must be applied with care to protect the privacy and safety of an affected person.

Example

Tom's grandmother calls the telco to restore the mobile service of her 16 year-old grandson who has left a domestic and family violence situation and is now living with her. The perpetrator (Tom's mother and the account holder) stopped paying for his mobile service which resulted in disconnection. Tom wants his previous mobile number reinstated to maintain contact with school, friends and support services.

Telco actions

After confirming it is safe to communicate, the telco works with Tom and his grandmother to reinstate the service. Instead of requesting evidence, the telco:

- accepts Tom's statement and prioritises restoring service in a way that safeguards his privacy and safety
- does **not** ask Tom to contact or engage with the perpetrator or the perpetrator's authorised representative
- uses alternative verification methods such as verbal affirmation or knowledge-based questions instead of documentary evidence
- offers safe options for reinstating the number, for example, transferring the number to a new account under Tom's name or his grandmother's account
- updates communication preferences to prevent disclosure to the perpetrator.

Tom receives support without needing to provide evidence of abuse. By relying on internal checks rather than documentation, the telco safeguards Tom's privacy and applies a trauma-informed response and enables the return of his previous number.

Example

Aisha contacts her telco seeking help with a large outstanding debt. She discloses that she is experiencing domestic and family violence and suspects her former partner has used multiple services under her name without her consent and is concerned that she will be liable for the debt.

Telco action

After confirming it is safe to communicate, the telco transfers Aisha to a trained domestic and family violence support specialist. Instead of requesting evidence, the specialist reviews internal account records and identifies:

- devices linked to Aisha's account
- usage patterns and locations inconsistent with her known address
- service changes that do not align with her typical behaviour.

Based on this information, the telco determines that there is a reasonable basis to support Aisha's claim of economic abuse. The telco:

- places a hold on credit management
- separates disputed services from her account
- initiates a financial hardship assessment
- flags the account for restricted access and updates communication preferences
- refers Aisha to external domestic and family violence and financial counselling services.

Aisha receives support without needing to provide documentation of abuse. The telco's internal records help validate her experience, protect her safety and ensure a trauma-informed response.

Can a telco ask an affected person if they are comfortable engaging with the perpetrator if that will speed up the matter to their benefit?

No. Telcos cannot ask an affected person to contact or engage with the perpetrator or the perpetrator's authorised representative for any reason. This includes asking the affected person if they are willing to do so to make things quicker or easier.

Example

Zara tells her telco that her ex-partner is abusive and forced her into signing multiple contracts which she cannot access or use. She now faces debt for services and devices, and requests support from the telco's domestic and family violence team to resolve the issue and remove her responsibility of the debt.

The telco must:

- not ask details of the abuse Zara has experienced
- provide the information to the domestic and family violence support team before transferring the call, so that Zara does not have to repeat her story
- ensure Zara is not asked to contact her ex-partner or their representative, even if doing so might expedite account or debt resolution.

How should a telco manage a transfer of a service and the rights of use (ROU) of the number of an affected person?

Under clause 4.3.3 of the Use of Numbers (UON) Code, telcos may treat domestic and family violence as a breach of terms and conditions. This allows for the disconnection of a number and removal of ROU from the perpetrator (customer), enabling reissuing of the number to the affected person (end user[4]).

Local number

If the affected person is the 'customer' or the 'end user', services can be moved to a new account following standard procedures.

Mobile number

If the affected person is the 'end user' and the perpetrator is the 'customer', telcos must have processes to:

- terminate the perpetrator's ROU to the number
- disassociate the number from the perpetrator's account
- transfer the number to the affected person's new account.

Under clauses 4.7.2 and 4.7.3 of the UON Code, telcos may remove and reissue a quarantined number to an affected person – either a former customer or authenticated end user – before the standard 6-month quarantine period.

Telcos should review and modify their Standard Form of Agreement to ensure it allows for the termination and disassociation of a mobile number from accounts where domestic and family violence has occurred.

Example

Kathy experienced years of emotional and financial abuse. Her phone number – linked to her husband's account – was her main connection to family, support services and essential services including government services and her bank. After she left the relationship, her husband called the telco and had her number blocked so she could not make or receive calls or messages.

Telco action

The telco worked with Kathy to restore her service by transferring the number to a new account in her name. It also provided domestic and family violence support and guidance to help Kathy keep the account and service safe and secure.

[4] *End user means the consumer using a telecommunications product who is not a customer.*

How does a telco deal with the former ROU holder (the perpetrator)?

When action is taken to reissue a number due to domestic and family violence, telcos may need to respond to the former ROU holder (the perpetrator), noting that this needs to be consistent with applicable privacy obligations.

Staff guidance

Telcos should provide clear instructions to staff, including:

- **No disclosure of domestic and family violence context**: Under no circumstances should staff inform the former ROU holder that the termination of service was related to domestic and family violence.

Suggested neutral responses:

If the former ROU holder asks why the service was terminated, staff should respond with neutral statements that do not reveal domestic and family violence or personal details. For example:

*"*The service has been closed in line with our account management processes."

"We're unable to provide details about the reason for closure, but we can assist you with options for a new service if you'd like."

"The account is no longer active. If you'd like to discuss setting up a new service, we can help with that."

"We can't share specific details about the previous account, but we're happy to help you with next steps."

- **Account notation**: A note should be placed on the account stating that the ROU has been terminated. Any future charges (such as early termination fees or porting costs) associated with the number from the termination date should be waived to ensure the affected person isn't billed for anything related to the cancelled service.
- **Staff support**: Frontline staff must have access to appropriate support if the former ROU holder escalates or engages in aggressive or abusive behaviour.

What must telcos tell consumers about domestic and family violence support while policies and procedures are being developed to comply with the Standard?

Telcos need to have accessible DFV statements published by 1 January 2026 for large telcos and 1 April 2026 for small telcos.

While telcos are preparing these statements, they are required to publish information (from 1 July 2025) on their website about:

- any domestic and family violence support that it currently offers
- how an affected person can access that support.

If telcos don't offer specific domestic and family violence support, then they must publish information on their website which includes:

- where people can direct their requests for support
- the date when the telco will have more support in place
- contact details for a domestic and family violence support organisation.

Part 4 – Requirements relating to availability of domestic and family violence support information

What domestic and family violence support information does a telco need to publish (section 16)?

Telcos must publish clear information on their website about the support they offer to people affected by domestic and family violence. This requirement applies whether or not the telco provides its own domestic and family violence support services.

If a telco does provide specific support, they must publish:

- what support is available
- how the affected person can access it.

If a telco **does not** offer specific support, they must still publish:

- where people can direct their requests for support
- information and contact details of one or more external support organisations that the customer can contact
- information about when their support services will become available.

Organisations across different sectors have published strong examples of domestic and family violence information. For example, the National Australia Bank and Insurance Australia Group clearly outline available domestic and family violence support options and safety features for affected customers.
These are provided as examples only and do not imply endorsement.

What are 'organisations'?

1800 RESPECT meets the 'organisations' test for the purposes of paragraph 16(2)(a). Other organisations (and their phone numbers) which might help an affected person are listed in the Standard under 'support telephone numbers' (section 5) and include:

- 1800 ElderHelp: 1800 353 374
- Full Stop: 1800 385 578
- National Debt Helpline: 1800 007 007
- National Disability Abuse and Neglect Hotline: 1800 880 052
- Rainbow Sexual, Domestic and Family Violence Helpline: 1800 497 212.

Telcos can find other state and national support services at Find a service - Are You Safe at Home?

Do telcos have to consult with 'organisations' when developing domestic and family violence website information?

No. Telcos are not required to consult with organisations when developing DFV support information on its websites. However, telcos may choose to use content from their DFV policy and procedures – developed in consultation with organisations and experts as required under section 32 of the Standard – to help shape and strengthen its website information.

What does a 'clearly available' domestic and family violence statement mean (paragraph 17(3)(f))?

'Clearly available' means a DFV statement that is easy to find on the homepage or mobile app and clearly titled with words including 'domestic and/or family violence' in a visible font size.

It does not mean making the DFV statement available under a general heading of support at the bottom of the webpage or a 'contact us' button or a link to a general help centre.

Part 5 – General requirements relating to policies and procedures

Is a telco required to develop domestic and family violence policies and procedures?

Yes. Telcos must develop and implement policies and procedures that explain how they will support and interact with affected persons. They also need to develop clear procedures for staff to follow, ensuring minimum requirements in the Standard are met.

What are the minimum requirements for a telco's domestic and family violence policy (subsection 20(1))?

A telco's DFV policy must be in writing and prioritise the safety of the affected person. It must set out:

- how it will support and manage affected persons
- types of assistance available to those customers
- what support is available for its staff who work with affected persons
- how an affected person's privacy and security will be protected, including how personal information is handled and stored in way to keep them safe
- how '**inclusive design'** will be used when developing and reviewing systems, processes and products – to help identify and reduce risks to affected people
- how an '**intersectional approach'** will be used to support consumers from diverse backgrounds, including those affected by non-domestic sexual violence.

What is 'inclusive design' and how would this be reflected in a policy?

Inclusive design means a telco creates its products, services and systems to be used as broadly as possible regardless of a person's age, ability and circumstances.

Unlike accessibility, which often focuses on compliance for people with disabilities, it goes beyond to embrace diversity and equity, so that no one is excluded or disadvantaged. It is important to understand that true inclusion is impossible without safety. For individuals experiencing vulnerability—such as domestic and family violence—safety is not just a feature; it is a prerequisite for access. Consultation with experts can help telcos develop or refine policies and procedures with this in mind. A telco's DFV policy must reflect how this is addressed in its systems, processes and products.

Examples of inclusive design

- Design for people with lived domestic and family violence experience, disability, elderly, or low literacy.
- Make safety features and information easy to find.
- Design websites and apps with adjustable text, screen reader support and simple navigation.
- Ensure stores and call centres are accessible.
- Use clear, plain language and provide support in different languages where possible.
- Use videos and translation for complex information.
- Train staff in inclusive, cultural awareness.
- Let customers choose their name, pronouns, and communication preferences (including where not required by law).

What is an 'intersectional approach' and **what are the risks/barriers for support (paragraph 20(1)(h))?**

An intersectional approach recognises how different aspects of a person's identity such as gender, race, disability, sexual orientation and socio-economic status interact and overlap to shape their experiences, particularly in relation to discrimination and disadvantage. It recognises that people don't experience oppression or privilege based on a single identity, but through multiple, interconnected factors.

This means a person's experience of domestic and family violence can be influenced by cultural, individual, historical, environmental or structural factors, including race, age, location, sexual orientation, ability or class.

Understanding intersectionality and how it can be a barrier to seeking and/or receiving support can help you better design your policies, procedures and training to provide effective and equitable responses to domestic and family violence.

Heightened risk factors

- **Women and children** are statistically more likely to experience domestic and family violence.
- **First Nations women** face significantly higher rates of violence, compounded by systemic racism and historical trauma.
- **People with disabilities** may be abused by carers or in institutional settings, with fewer pathways to report or escape.
- **LGBTQIA+ individuals** may face abuse within their homes and discrimination or exclusion when seeking help.
- **Migrant and refugee women** may be dependent on partners for visa status, face language barriers and lack social support networks.

Barriers to support

- Services not being culturally safe or inclusive.
- Language barriers, lack of interpreters or accessible formats.
- Discrimination (for example, racism, ableism, homophobia).
- Fear of legal or immigration consequences.
- Lack of awareness of domestic and family violence, especially where cultural norms discourage disclosure.

Unique experiences of violence

Some individuals may not identify their experiences as domestic and family violence due to cultural norms or lack of awareness.

Multiple layers of discrimination can compound harm. For example:

- An LGBTQIA+ First Nations person may face exclusion both within their cultural community and LGBTQIA+ spaces.
- A woman with a disability from a culturally diverse background may experience abuse from carers and struggle with language barriers when seeking help.

Example

A migrant woman from a Greek background with a speech impediment may rely on a carer who is also her abuser and manages her account. If customer support doesn't provide an interpreter or information in her language, she may be unable to request changes such as removing the abuser as the authorised representative or updating preferred communication methods, leaving her dependant and at risk.

What are the minimum requirements for a telco's domestic and family violence procedures (subsection 20(2))?

A telco's DFV procedures must be '**trauma informed'** (as explained below) and set out:

- how staff can safely and appropriately identify, support and assist domestic and family violence consumers and appropriately engage with perpetrators
- how staff will implement the requirements relating to security of personal and sensitive information under section 27
- how staff should manage and respond to domestic and family violence and, where relevant, non-domestic sexual violence, including:
  - what each staff member is responsible for
  - what escalation channels are available (for example, domestic and family violence support teams or managers)
  - when to escalate a case
  - providing support available to staff to assist affected persons
- how agreed actions with an affected person will be recorded in a way that keeps the information safe and confidential and prevents accidental disclosure to a perpetrator
- processes to minimise the number of times an affected person has to explain their circumstances, so they don't have to re-explain their situation to multiple staff members.

What does 'trauma informed' mean?

Trauma-informed means recognising that many people have experienced trauma, which affects their emotional, mental and social wellbeing and how they interact with services.

The way telco staff respond can either help a customer feel safe or cause more distress. In telecommunications, being trauma-informed means:

- Providing safe, clear ways consumers can raise concerns and request support that meets their individual needs.
- Communicating with empathy and respect and helping build trust.
- Minimising the risk of re-traumatising by not asking consumers to repeat distressing experiences or share unnecessary details.
- Prioritising safety, choice and control – helping consumers feel secure and empowered.

Examples of telco support that is trauma informed

- Draw on expertise from people with lived experience to directly inform systems and processes.
- Let customers choose how and when they're contacted.
- Offer discreet options, such as silent SMS or online chat, for customers at risk.
- Allow secondary contacts or safe words for secure identity checks.
- Train staff to refer consumers to specialist services, such as 1800RESPECT or local shelters.
- Offer flexible payment options or hardship programs.
- Offer multilingual and culturally appropriate support (for example, for First Nations peoples, migrants and refugees).
- Provide support for all genders, using inclusive language for LGBTQIA+ customers.
- Clearly explain how customer data is used and who can access it.
- Be upfront about steps taken after a domestic and family violence disclosure, including any reporting.

Part 6 – Training

When must telcos deliver domestic and family violence training for staff?

Telcos must ensure that all staff receive training on its DFV policy. This training must be delivered by the telco or by a qualified third-party individual or organisation that has domestic and family violence expertise:

- by **1 April 2026** for **large telcos** for existing personnel
- by **1 July 2026** for **small telcos**
- annually thereafter (from the date of the last training).

Who needs training?

All current staff (including contractors and customer-facing staff) must be trained. New staff must receive training within **one month** of commencing work with the telco. All staff are required to complete refresher training annually. Telcos are required to keep records of the training delivered, to whom it was delivered and when the training occurred. These requirements are set out in Part 9 – Record keeping of the Standard.

What types of third-party organisations have domestic and family violence expertise?

When considering third-party domestic and family violence experts, telcos must refer to the consultation requirements under Part 10 of the Standard, on who they must consult with.

When developing your training in consultation with your DFV experts, below are some resources for general information only:

- Fair Work Ombudsman – information about employer obligations in relation to domestic and family violence.
- 1800Respect – general information about domestic and family violence training and professional development.
- DV-aware – a free online workshop that provides an introduction to understanding domestic and family violence.
- e-safety – online resources for frontline workers focused on recognising and responding to tech-facilitated abuse in domestic and family violence contexts**.**

What domestic and family violence training is required for 'customer facing personnel' (section 22)?

Customer-facing personnel are staff who interact directly with consumers, particularly those handling general enquiries or working in areas where domestic and family violence issues may arise. This includes roles in sales, credit collections, financial hardship assistance, fraud investigation, privacy management and complaint resolution.

Telcos must ensure these personnel receive 'specialised DFV training', developed in consultation with domestic and family violence experts, which may be delivered by the telco or an external third-party individual or organisation with expertise in domestic and family violence. The training must equip staff with the skills to identify, support, and respond to affected persons safely and appropriately. Without this training, staff may inadvertently mishandle sensitive situations – such as by requesting evidence, breaching confidentiality, or failing to offer appropriate support – which can retraumatise affected individuals or discourage them from seeking help again.

What must specialised domestic and family violence training cover?

This training should cover issues which help staff understand and apply the telco's DFV policy and procedures, including recognising signs of domestic and family violence and understanding how it affects a person's ability to engage with telco services. It must also cover how personal factors – such as age, culture, disability, or financial situation – can shape a person's experience and support needs.

The training should equip staff to respond sensitively and safely when a customer's circumstances change, and to manage interactions where a perpetrator may be involved. It must also include guidance on privacy and confidentiality, warm transfers to support services and role-specific scenarios to ensure staff avoid actions that could retraumatise affected persons.

When providing organisation-wide training to staff, what is meant by personnel who are 'indirectly' involved with consumers?

Organisation-wide training should extend beyond frontline and customer-facing staff to include personnel who may be indirectly involved in supporting affected persons. This includes:

- senior and upper management staff
- product and systems developers whose design choices can impact safety and privacy
- information technology teams who manage data security and access controls
- human resources staff who support staff wellbeing.

It is **not** expected that roles without an association or influence over the outcomes for consumers in Australia receive training – for example, office cleaners or building maintenance staff.

Can telco staff opt out of domestic and family violence training?

Telcos are required under the Standard to ensure staff complete DFV training (sections 21 and 22). While the Standard does not provide for staff to opt out of training, telcos would still need to meet their obligations under workplace health and safety (WHS) laws – including protecting their staff's psychological wellbeing. For example, if a staff member has lived experience of domestic and family violence and cannot safely participate, the telco should manage this under its WHS framework, not as an exception to the Standard. For example, the staff member may be excused from all or part of the training if participation would cause harm, however the telco should document this as a WHS issue.

Part 7 – Monitoring and review

How often do telcos need to review their domestic and family violence policy?

Telcos must review their DFV policy and procedures:

- at least once every 24 months, to ensure they remain fit for purpose
- sooner if needed – for example, if the policies appear not to be protecting the safety of an affected person.

Current timeframes indicate that reviews must be conducted by:

- 1 January 2028 for large telcos
- 1 April 2028 for small telcos.

Telcos will not meet this requirement if the required domestic and family violence expert consultation under Part 10 has not been completed. Failure to do so constitutes a breach of the Standard and may result in enforcement action by the ACMA.

How can a telco identify when domestic and family violence policies and procedures may not be operating effectively and not protecting the safety of an affected person?

Under paragraph 23(b), telcos must review and update their domestic and family violence policy and procedures if they become aware that they are not effectively protecting the safety of affected persons.

Indicators that may trigger a review include:

- **consumer complaints** – particularly those raising safety concerns or systemic issues
- **feedback from advocacy organisations** – including domestic and family violence support services
- **systemic analysis outcomes under the Complaints Standard** – which may highlight patterns of harm or risk
- **internal monitoring** – where staff feedback suggests procedures are not being followed or are causing unintended harm
- **compliance action** – by the ACMA or other regulators, especially where there is evidence of impact on a person affected by domestic and family violence or broader customer groups.

Telcos should have internal processes to monitor these indicators and act promptly when concerns arise.

What does 'as soon as practicable' mean (subsection 24(5))?

Telcos must act 'as soon as practicable' to update their DFV policy and procedures when they become aware of issues affecting the safety of affected persons.

This means:

- acting promptly and reasonably, based on the seriousness of the issue
- prioritising customer safety over business-as-usual timelines.

It does not mean:

- waiting until the next scheduled review cycle
- delaying action for commercial convenience or operational ease.

Part 8 – Security and privacy

How can telcos protect the security and privacy of an affected person?

A telco must not, without the affected person's consent, disclose to any other person any personal or sensitive information about them (unless required by law) which can be used to identify or locate them, including their:

- **contact details** – such as phone number, email or address
- **financial information** – such as billing details or account history.

Customer information must be stored securely and protected from misuse, interference, loss or disclosure to a perpetrator.

Example

Jesse contacts their telco to update account details, including providing a new contact email address, after relocating to a safe address. Jesse is concerned about her perpetrator locating her. The telco reassures her that her new details are secure.

Good practice protocols

Domestic and family violence privacy protocols to protect the customer's safety and confidentiality include:

- **restricted access** – only authorised staff can view or modify Jesse's personal information
- **access logs** – there are logs to show who accesses Jesse's account and when
- **address suppression** – the physical address is suppressed across all systems
- **billing protections** – supressing data usage details, removing location specific information and ensuring bills are sent only to secure contact points (like a new email address)
- **communications controls** – Jesse's preferences are updated across all systems to ensure safety
- **system safeguards** – checks are in place before issuing communications to prevent accidental disclosure
- **verification and audit** – the telco confirms all privacy and security protocols have been correctly applied across systems and interactions, ensuring Jesse's information remains protected.

Where should the quick exit function appear on a telco's website (subsection 25(2))?

Telcos must provide a quick exit function – a prominently displayed button – on all webpages that relate to support for affected persons. This function enables users to immediately leave the site and redirect to a neutral webpage, helping protect their privacy and safety.

The quick exit function must:

- be clearly labelled 'Quick Exit' and placed at the top of all relevant webpages regardless of the device used (for example, desktop, mobile phone, tablet)
- redirect instantly to a neutral site (for example, https://www.bom.gov.au or a google search page) with one click.

While not required, the following features are recommended to enhance usability and safety:

- avoid leaving a trace in the browser history, where technically feasible
- be keyboard-navigable and compatible with screen-readers.

For example, see the quick exit function on website Safe Steps Family Violence Response Centre – a Victorian organisation offering 24/7 crisis support for people experiencing family and domestic violence.

Can telcos use flags on domestic and family violence accounts to identify affected persons?

Telcos may use internal flags to help identify and support customers who need extra privacy or protection, but these flags should be used carefully to avoid putting a customer at risk.

Flags can help by letting staff know that a customer needs extra care. However, if not handled properly, flags can accidentally reveal private and confidential information (for example, if visible in customer-facing systems used by retail staff in stores) and be misused or misunderstood by staff who aren't trained – which can cause distress or harm if the customer didn't agree to it.

Telcos should:

- consult with domestic and family violence experts before setting up a flagging system
- get informed consent from the customer before applying a flag
- use neutral language such as 'privacy support required' – never mention domestic and family violence directly
- ensure only authorised staff can see or use the flag
- train staff on how to use flags safely and discreetly, including how to use them in conversations and systems.

Do telcos need to keep records of support telephone numbers that are hidden from bills (subsection 25(3))?

Subsection 25(3) requires telcos to suppress support telephone numbers on any bills or other documents issued to affected persons (to protect their privacy and safety), but it does not require telcos to keep internal records of calls or messages made to those support telephone numbers. However, if a telco has the technical capability to retain such records securely, they are encouraged to do so to support legitimate purposes such as investigations or court proceedings.

If privacy is breached, how do I notify the affected person and the ACMA (subsection 29 (1))?

If personal information is accessed or shared without permission, telcos must notify the customer and the ACMA within **2 days** of becoming aware of the breach. This includes circumstances caused by human error, malicious intent or cyber-attacks.

Telcos must have systems and processes in place to detect privacy breaches, assess the impact (especially if an affected person may be at risk) and how breaches must be handled.

Notifying customers

Telcos must use the agreed safe communication method. Telcos must not use alternative methods, even if it's faster (as this may put the affected person at risk of being contacted or located by the perpetrator).

If the agreed method is only available on certain days (for example, Wednesdays) and the breach occurs outside that window, the telco must notify the affected person using the agreed method as soon as practicable. The telco should also take steps to reduce risk until the notification can occur.

The notification should explain what information was breached and offer support, including a referral to a national or state based domestic and family violence support service for safety planning. The notification should also provide options to change account settings, suppress information or take protective steps.

For example, if a customer has asked to be contacted by email, do not call them by phone – even to notify them of a breach.

Notifying the ACMA

Telcos must notify the ACMA details of the breach and support provided to the affected person via email dfvprivacynotifications@acma.gov.au or telephone 1300 850 115. Templates to assist telcos with notifications are provided at the following links:

- Individual Privacy Breach Notification template
- Multiple Privacy Breach Notification template

Do telcos need to notify affected people about all data breaches under the Standard?

Yes. Telcos must notify affected persons if their personal information is accessed or disclosed without permission – even if the breach appears to be minor.

This differs to the notifiable data provisions in Part IIIC of the Privacy Act 1988, which only requires notification if the breach is likely to cause serious harm to an individual.

While a telco may consider a data breach to pose low or minimal harm, the telco must still notify the affected person. Each affected person's circumstances are different. The affected person may well be placed at risk where the telco assesses the data breach as 'low risk', but it is not a low risk for that individual in their circumstances. The affected person should be notified of the breach and allowed to assess whether it poses a low risk for them. This affords the affected person the opportunity to take any additional protections they think is necessary for their safety.

Example

A staff member at a telco accesses a customer's support interaction history without authorisation but there is no evidence of misuse of the information.

Assessment

The telco considers the breach low risk because the data was not disclosed externally, and no harm occurred.

Why notification is required

The affected person may feel unsafe knowing their information was accessed without permission, and there may be concern that the perpetrator socialises with a staff member of the telco. Notification empowers them to raise concerns or request additional privacy measures.

What does 'personal information' mean under Part 8? Does it refer to the definition in the *Privacy Act 1988*, or is it limited to information collected under this Part?

Personal information is any detail that can identify a person or could reasonably be used to identify them directly or indirectly, from the information itself or from that information combined with other information. This includes information such as names, addresses, phone numbers, account details, an IP address, biometric data, location from a mobile device and even notes or opinions about someone – whether written down or not, and whether true or not.

Under Part 8, personal information should be interpreted in line with the Privacy Act. The Privacy Act defines personal information as:

> Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

It is not limited to information collected under Part 8 of the Standard. Instead, it covers all personal information held by a telco about an affected person, regardless of how or when it was collected. Telcos should treat this information as private and confidential personal information and apply strong privacy and security protections across all systems and interactions.

Part 9 – Record keeping

What are the record keeping and retention rules for telcos?

Telcos must keep records that show they're following the rules in the Standard. Telcos must:

- only collect necessary information
- protect information from misuse, interference and loss, unauthorised access, modification and disclosure
- ensure information is safely disposed of and destroyed when it's no longer needed.

Telcos are required to keep records for a minimum of 2 years or for as long as the affected person receives support under the Standard and make records available to the ACMA upon written request. Where practical, records must not contain personal information of the affected person.

Customer complaints records must be held for longer (the 2 years plus 12 months after the complaint is resolved).

Where a telco requests and receives evidence to meet a legal obligation, the telco must only retain a copy of the record for the duration necessary to meet the legal obligation and dispose of or destroy the material securely once the obligation has been met.

Some examples of different record keeping methods for different requirements are set out in the table below.

Requirement	Suggested record keeping method
Customer disclosure of domestic and family violence	Summarise interaction without storing unnecessary details. Note date and staff involved; use neutral or coded language.
Evidence	Notation where sighted and verified by trained staff. Securely destroyed after use.
Agreed communications method	Record agreed communication method and any updates or changes.
Authorisation request	Retain signed request or consent form, this may include an email or recording if verbal consent was given.
Internal staff notes on domestic and family violence case handling	Use coded language or summary notes. Avoid detailed descriptions of abuse.
Service adjustment due to domestic and family violence	Retain records of changes (for example, billing adjustments, service restrictions lifted).
Advised of domestic and family violence policy and third-party support	Tick box in CRM.
Staff training records	Retain certificates or logs confirming DFV training for compliance audits.
Domestic and family violence flag activation log (if used)	Retain system-generated log showing flag activation, date, and staff ID.

Part 10 – Consultation

Which domestic and family violence services or organisation would meet the requirements to consult?

When developing or reviewing domestic and family violence materials, telcos must consult with:

- A national or state-based domestic and family violence support service or organisation, such as:
  - WESNET – technology-facilitated abuse and privacy expertise
  - Our Watch – a national leader in domestic and family violence prevention
  - White Ribbon – offers workplace accreditation and respectful culture tools
  - WIRE – domestic and family violence training and support for women.

Telcos must also consult with either:

- **A panel of people with lived experience of domestic and family violence, or their representatives**, such as:
  - Safe and Equal – lived experience, community awareness and advocacy consultancy
  - Thriving Communities Partnership – cross-sector collaboration and lived experience via the One Stop One Story Hub.

Note: 'A panel of people with lived experience' means a minimum of 2 or more people with lived experience of domestic and family violence. Ideally, these people should be consulted with the support and guidance of a domestic and family violence organisation or service with experience in advocacy. 'Their representatives' refers to someone within a domestic and family violence advocacy organisation who has consulted directly with those with lived experience on the telco's behalf.

Or:

- **A national or state-based organisation representing disproportionately affected groups** – such as First Nations people, people with disability, culturally and linguistically diverse communities and LGBTQIA+ individuals, such as:
  - Economic Abuse Reference Group (EARG) – financial abuse and referral guidance
  - Good Shepherd Australia & New Zealand – tailored programs and training for vulnerable communities
  - Uniting Kildonan – consultancy and training for organisations supporting vulnerable customers
  - First Nations Advocates Against Family Violence – advocacy and support for Aboriginal and Torres Strait Islander communities
  - ACON (AIDS Council of NSW) – LGBTQIA+ health and domestic and family violence support.

Consultation may be undertaken through a single 'gateway' organisation who offers access to some or all these experts, such as Thriving Communities Partnership.

Can telcos use existing domestic and family violence policies from other sectors?

Yes, telcos can use existing policies and resources from other sectors to help develop or review their own DFV policies and materials. Using well-established policies can help support the creation of informed procedures, align with best practice and provide a strong foundation for meaningful consultation. Existing resources may include internal policies, industry templates or materials developed in collaboration with domestic and family violence organisations.

Can telcos use the same domestic and family violence policies?

Yes. Telcos, particularly **smaller telcos**, can adopt existing DFV policies (for example from larger telcos) to reduce duplication and resource burden. Smaller telcos may choose to consult directly through an industry body to streamline its policies.

Examples include:

- Telco Together Foundation – DFV Action Framework – provides tools and resources tailored to the telecommunication sector, and can connect telcos with domestic and family violence experts, lived experience representatives and advocacy groups. The framework includes example policies, training materials and consultation guidance.
- Industry Impact Hub – offers guidance on how to better support its customers and includes a comprehensive document *Telco Industry DFV Action Framework* to help telcos develop their action plans.
- Australian Telecommunications Alliance (ATA) – may facilitate sector-wide consultation.

When engaging through a representative organisation, it is important that the consultation is relevant to the telco's customer base and operational context.

How do telcos ensure domestic, family and sexual violence materials are sufficient?

Telcos can ensure their domestic, family and sexual violence materials are sufficient by applying a combination of expert validation, user testing and ongoing review. Key steps include:

- **Consultation with domestic and family violence experts and people with lived experience** – materials could be reviewed by individuals or organisations with specialist knowledge in domestic and family violence, trauma-informed practice and consumer safety. This ensures content is accurate, sensitive and aligned with best practice.
- **Testing with frontline staff and affected consumers** – where appropriate, telcos can test materials with staff and/or consumers to assess clarity, accessibility and practical usefulness. Feedback should inform improvements.
- **Alignment with the Standard and Privacy Act** – materials should be checked against the requirements of the Standard and relevant privacy obligations under the Privacy Act to ensure compliance. If there are inconsistencies between obligations, telcos should comply with the requirement that imposes the strictest obligation. For example, the Standard currently imposes higher obligations regarding data breach notifications than the Privacy Act.
- **Internal review and quality assurance** – telcos should establish internal processes to regularly review domestic, family and sexual violence materials, especially following updates to legislation, feedback from stakeholders or incidents that highlight gaps.

- **Participation in industry-wide consultation** – smaller telcos may benefit from shared consultation processes coordinated by industry bodies, with materials tailored to their operational context.

Can I use the ATA's domestic and family violence guideline to fulfil the requirements for consultation?

No. Telcos must consult with the relevant experts as outlined in subsection 32(1) of the Standard. These are:

- a national or state-based domestic and family violence support service or organisation; and
- either a panel with lived experience or a national or state-based organisation representing a group disproportionately affected by domestic and family violence.

However, the ATA's superseded domestic and family violence guideline (G660:2023 Assisting Consumers Affected by Domestic and Family Violence - Australian Telecommunications Alliance) could be used as a resource in developing draft policies, procedures and specialised training before consultation with the relevant experts.

Can telcos refer to guides developed in other regulated sectors?

Yes. Telcos may find it helpful to refer to guidance developed by domestic and family violence experts and affected communities across other regulated sectors to see how consultation has been embedded into policy development, staff training and customer support frameworks.

Examples include:

- Australian Energy Regulator (AER) for electricity and gas retailers.
- Australian Banking Association (ABA) for financial institutions.
- Essential Services Commission (Victoria) for water businesses.

Part 11 – Conferral of functions and powers

What role does the Telecommunications Industry Ombudsman (TIO) play?

The TIO can assist consumers experiencing domestic, family, or sexual violence if they cannot resolve issues directly with their telco. The TIO has powers to receive, investigate, resolve, make determinations, issue directions, and report on complaints about matters covered by the Standard. Telcos must cooperate and comply with its decisions.

What should telcos do when the TIO requests personal information during a domestic and family violence-related complaint?

When the TIO is investigating or resolving a complaint under the Standard, telcos may be required to disclose personal information to the TIO.

Telcos must carefully assess the safety risks before sharing personal information. They should:

- only share what's necessary to resolve the complaint
- avoid disclosing private and confidential details that could put the affected person at risk
- where safe, confirm with the affected person that they agree to the information being shared
- keep records of what was shared and why.

How can telcos protect a person affected by domestic and family violence when a complaint is handled via an Authorised Representative?

Telcos should take extra care when a complaint is made through an Authorised Representative to ensure the safety and privacy of the affected person. Recommended steps include:

- confirming the representative is legitimate and not connected to the perpetrator
- checking with the affected person, where safe and appropriate, to ensure they consent to the representative's involvement
- raising concerns with the TIO if there's any risk to the affected person or their representative, and work with the TIO to ensure the complaint-handling processes prioritise safety.

These steps help ensure that complaint processes do not inadvertently compromise the safety of individuals affected by domestic, family and sexual violence.

Further information

Does the DFSV Standard set timeframes for handling complaints?

No. Complaint handling timeframes, including urgent complaints, are set out in the Complaints Standard. From 1 January 2026, all telcos must treat complaints as ***urgent*** where the affected person indicates a threat to their safety and/or their children.

These complaints must be resolved within **2 working days**, in line with the updated Complaints Standard rules.