Australian Government

Disability Employment Services

Servicing Participants with Challenging Behaviours Guidelines

V1.3

Disclaimer
This document is not a stand-alone document and does not contain the entirety of Disability Employment Services Providers' obligations. It should be read in conjunction with the Disability Employment Services Grant Agreement and any relevant guidelines or reference material issued by the Department of Social Services under or in connection with the Disability Employment Services Grant Agreement.

Table of Contents

Document Change History

Version	Effective Date	End Date	Change & Location
1.3	09 March 2020		Remove Department of Human Services or DHS and replace with Services Australia.
1.2	1 July 2019		General restructuring of document. Introduction of Managed Service Plans.
1.1	3 December 2018	30 June 2019	Change of terminology from Account Manager to Relationship Manager to reflect Direction No: 2.
1.0	1 July 2018	2 December 2018	Original version of document

Background

These Guidelines provide information for DES Providers on the servicing of Participants with challenging behaviours. They also set out requirements for, and provide information about, lodging Incident Reports in the Department's IT Systems when servicing Participants with challenging behaviours.

DES Providers need to adapt the strategies that are outlined here to suit their particular circumstances. These Guidelines should supplement, not replace, existing internal operational policies and procedures. DES Providers are responsible for informing themselves of their legal obligations and taking appropriate measures to comply with obligations.

Disability Employment Services Grant Agreement Clauses:

Clause 75.1(a) – Compliance with laws and government policies.
Clause 80.1 – Provision of Program Services
Clause 106 – General requirements for a Job Plan

Explanatory Note:

All capitalised terms have the same meaning as in Disability Employment Services Grant Agreement.
In this document, "must" means that compliance is mandatory and "should" means that compliance represents best practice.

Policy Intent

The aim of the policy is to provide DES Providers with guidance on how to continue delivering services to Participants with challenging behaviours without risking their staff, Participants or property, while ensuring that Participants meet their Mutual Obligation/Compulsory Participation Requirements and remain connected with services. These Guidelines also assist DES Providers to identify and report challenging behaviours that Participants may display.

Providers need to adapt the strategies that are outlined here to suit their particular circumstances. These Guidelines should supplement, not replace, existing internal operational policies and procedures. Providers

are responsible for informing themselves of their legal obligations and taking appropriate measures to comply with obligations.

1. Recognising Challenging Behaviour

Challenging behaviour is any behaviour that a reasonable person would consider unacceptable or hostile and that creates an intimidating, frightening, threatening, offensive or physically dangerous situation in the workplace or other location.

Challenging behaviours may include but are not limited to:

- physical violence against any person – for example hitting, kicking, punching, spitting on or throwing objects at a person
- acting in a way that would cause a person to have a reasonable belief that assault was intended
- adopting a physical position or state and/or producing an object that a reasonable person would consider constitutes a serious and imminent threat of physical violence
- oral or written (including email or communication through social media) threats
- abuse or harassment, inappropriate touching or stalking staff members
- damaging, defacing or destroying property intentionally or through inappropriate and aggressive behaviour, such as throwing objects or punching and kicking property
- theft of property, illicit drug taking on DES Provider premises, use of DES Provider equipment and/or property for illegal purposes
- swearing, making offensive noises or gestures, inappropriate or suggestive comments, vilification
- threatening suicide; causing injury to oneself - for example cutting
- any other behaviour that is deemed inappropriate and warrants an incident being recorded

2. Managing the Challenging Behaviour Incident

General considerations

The Department acknowledges that that the safety of Providers and Participants is a priority and that DES Providers have a wide variety of expertise and arrangements in place to address challenging behaviours. Strategies will differ between DES Providers and sites. Participants' circumstances differ and there may be a number and range of factors that contribute to incidences of challenging behaviour. Consideration of the contributing factors/barriers need to be explored before Providers consider applying servicing restrictions through a Managed Service Plan (see 'Managed Service Plans (MSPs)').

Examples of factors DES Providers could consider include the following:

- Whether the Participant has Mutual Obligation Requirements or other compulsory participation requirements, or whether the person is participating voluntarily
    - As set out in the DES Program Review, Program Summary and Exits Guidelines, a volunteer Participant can be exited if they are not participating appropriately in their program.
- Any Participant history, for example; a death in the family, carer's responsibilities, mental illness (past or present) and drug or alcohol dependencies (past or present).
- Whether the Participant has disclosed information or is displaying a behaviour and/or has displayed similar behaviour in the past that may warrant:
    - a referral for a new Employment Services Assessment (ESAt) or Job Seeker Classification Instrument (JSCI) reassessment due to a change of circumstances; or
    - a review conducted by Services Australia to ensure the Participant is on the appropriate payment type.

If Providers are unable to conduct a JSCI reassessment or make a referral for a new ESAt, they should discuss with their Relationship Manager.

When Providers are dealing with a case of challenging behaviour, they may wish to apply a Provisional (1-10 days) MSP to give time to consider any contributory factors. A Provisional MSP can provide a cooling off period to manage risk or deescalate behaviour and may also assist Providers in determining whether a Longer term MSP should be applied (see 'MSP Timeframes').

Completing a compulsory incident management plan

DES Providers must have an incident management plan in place that outlines the organisation's approach to managing situations where Participants display challenging behaviours, or where staff identify that a situation has the potential to result in this behaviour.

Where challenging behaviour is observed, Providers should consider whether police involvement is required and are encouraged to contact police if they believe it is necessary.

Temporary Site Closures

Where DES Providers experience incidents involving Participants with violent, aggressive or threatening behaviours, they may elect to temporarily close the affected site until the situation is resolved or until they are satisfied that the threat no longer exists.

The duration of closures will be determined on a case by case basis. Where sites are closed for an extended period, alternative servicing arrangements may be required.

Where sites are closed, at a minimum, Providers are required to:

- Notify their Relationship Manager as soon as practical (within 24 hours) following the decision to temporarily close a site.
  - This notification may initially be either over the phone or by email, but must be followed by formal written advice (within 24 hours).
  - This advice must also include details of any alternative servicing arrangements that have been put in place.
- Provide ongoing advice to their Relationship Manager regarding the situation, including estimations of when sites will reopen, and any mitigation strategies that have been required.
- Notify their local Services Australia/Centrelink office as soon as possible after the incident if the DES Provider feels there is a threat to Services Australia, otherwise within 24 hours.

💻 **System step**: DES Providers must record all incidents where a Participant exhibits challenging behaviour in the incident report screen in the Department's IT system, including where it has resulted in a site closure. [*DES Grant Agreement clause 75.5]* (see 'Completing incident reports').

Note: Under the *Freedom of Information Act 1982*, a person has the right (with limited exceptions) to access information or documents held by the Department or the Departments' contracted service providers.

Immediate notification requirement

Where an incident has occurred and the Provider has reason to believe that the Participant who is displaying threatening, aggressive or violent behaviour poses an imminent threat to another organisation, they should immediately contact the police and advise them of the situation, noting Public Interest Certificate (PIC)/Class PIC requirements (see 'Disclosing personal information').

Where a Participant has made threats towards Services Australia staff or Services Australia Service Centres, it is essential that these threats are escalated immediately to keep Services Australia staff and other Services Australia customers safe. In the first instance, Providers should attempt to call the Service Centre (the office closest to the Provider's location or the location of a threat) to advise them of the risk.

If Providers are unable to contact the Service Centre or are not sure who to call, they should phone the Services Australia Security Hotline on 1800 046 021. This hotline is managed by Services Australia Regional Security Advisers (RSA) and is operational nationally between 7.00 am and 7.00 pm. The RSAs will ensure that the issue is escalated appropriately.

In the event of an emergency – call 000.

Disclosing personal information

Personal information, including sensitive information, should be handled carefully and afforded a greater level of protection from unnecessary disclosure to third parties. Before disclosing a Participant's personal information to a third party, Providers should refer to the Privacy Guidelines. (*DES Grant Agreement clause 41*).

Information held about Participants may be both personal information under the Privacy Act and protected information under social security law.

Releasing protected information to a third party (including the police) using a Public Interest Certificate (PIC)

Protected information is a Participant's personal information, including names and addresses, obtained for administering the social security law.

Under the social security law, the Secretary of the Department of Social Services can issue a PIC, which allows disclosure of protected information.

A PIC identifies the information that can be released about a Participant; who it can be released to; who can release the information; and allows the information to be released.

Except in specific circumstances covered by the Class PIC below, Providers will need to approach the Department through their Relationship Manager to arrange a PIC from the Department to cover the release of protected information.

Class PIC

The Secretary of the Department has issued a Class PIC that authorises specified senior staff (i.e. site manager or above) working for DES Providers to disclose protected information only where there is a threat to someone's life, health or welfare (Threats).

In the case of Threats, the protected information can only be released to: emergency services (including the police); health service Providers; and child protection agencies.

For more information, please refer to the Privacy Guideline.

---

3. Incident Reporting and Post Incident Servicing

As part of the July 2019 Department's IT system release, processes for incident reporting and post incident servicing arrangements have changed.

The changes aim to make Participants' experiences more consistent across agencies by aligning processes and terminology for managing challenging behaviour with those used by Services Australia. This is through the use of:

- an **Incident Severity Matrix** - this is an automated process to assign a severity level to an incident. The matrix removes subjectivity when determining the severity of an incident based on key, factual information about the incident. Use of the matrix takes into account the importance of all incidents being considered in the context of 'organisational tolerance' not 'personal tolerance' and;
- **Managed Service Plans (MSPs)** – this process replaces the previous Case Management Plans (CMPs) and Restricted Servicing Arrangements (RSAs).

Completing incident reports

Incident reports are intended to record incidents, inform Providers and Services Australia frontline staff of the potential for further incidents and support compliance measures where appropriate.

By recording incidents, staff are informed about the history of challenging behaviour and potential for further incidents. The record also assists with determining appropriate future servicing arrangements. Accurate recording of incidents will also ensure that, if the Participant is transferred to another Site or Provider, the receiving Site or Provider is aware of the challenging behaviours and can arrange to service the Participant accordingly.

💻 **System step:** DES Providers must record all incidents where a Participant exhibits challenging behaviour in the incident report screen in the Department's IT system. Incidents should be recorded on the day the incident occurred or as soon as possible within 24 hours. Where it is not possible for the staff member who witnessed the incident to record the incident another staff member should record on their behalf.

💻 **System step:** Using the Incident Severity Matrix, the IT system will pose questions to the Provider about the incident and, based on the responses, will automatically assign one of three severity levels.

- Low Severity: An incident of behaviour that is a low risk to the health and safety of staff, property and others. A verbal warning or a warning letter may be issued.
- Moderate Severity: An incident which puts the health and safety of staff, property and others at risk. Incident requires follow-up, and may require escalation. A Managed Service Plan should be considered.
- Serious Severity: An incident which places the health and safety of staff, property and others at serious risk. Incident requires follow-up and must be escalated to the Relationship Manager if there is a Temporary Site Closure (see Temporary Site Closures). A Managed Service Plan, including restrictions on access to services, is likely to be applied.

💻 **System step:** Note: Providers can also use the Department's IT system to view details of incident reports and MSPs lodged by Services Australia. The above incident severity levels are the same for Services Australia and Provider lodged incidents.

💻 **System step:** The Incident Report Alert in the Department's IT system displays the number of active incident reports recorded against a Participant in the previous 24 months and provides a visual indicator of potential risk. The incident alert is activated at the time the user selects the Participant's record, and will display (if in place) the existence of a Managed Service Plan.

💻 **System step:** Note: Providers can view incident reports lodged prior to the July 2019 Department's IT system changes. As per the previous process, these will appear at the following three levels in Department's IT system:

- ES Level 1 - No police involvement but incident was recorded to ascertain a pattern of behaviour.
- ES Level 2 - Participant was not threatening, aggressive or violent (could include theft, inappropriate behaviour). Police may have been contacted and/or attended.
- ES Level 3 - Participant has shown threatening, aggressive or violent behaviour or has threatened to harm themselves or others. Police may have attended.

Managed Service Plans (MSPs)

MSPs are plans Providers can put in place to tailor the way services are delivered to Participants who display challenging behaviours.

MSPs prioritise the safety of staff and Participants while ensuring Participants stay connected to employment services to meet their Mutual Obligation or compulsory participation requirements.

An MSP can be applied at any time where it is considered by the Provider to be appropriate.

Key steps before applying an MSP

Generally, following an incident and prior to an MSP being applied, Providers should, where possible, discuss the Participant's behaviour with them and warn them of the implications of that behaviour. This will ensure that the Participant is given an opportunity to improve their behaviour before an MSP is put in place. This can be done verbally or in writing. Any warnings given to a Participant must be recorded on the comments screen on the Participant's record in Department's IT system.

Before Providers decide whether to apply an MSP and the type of MSP and timeframe, they must take into account:

- the incident severity;
- contributing factors including the Participant's personal circumstances;
- the time needed to address issues (e.g. A Participant may only require a 'cooling off' period and therefore a Provisional MSP could be applied); and
- the importance of ensuring the Participant remains connected to services.

(see 'General Considerations')

Types of MSPs

There are two types of MSP:

Reactive – following a challenging behaviour incident (a reactive MSP can only be put in place once an incident report has been recorded in the system), or

Proactive – where there has not been an incident but the Provider assesses that a Participant has identified vulnerabilities or barriers that may increase the risk of an incident.

An example of a Proactive MSP might be where a Participant has presented to a Provider site intoxicated on a number of occasions, without causing any incident. While an incident has not occurred, the Provider might assess that there is a risk of one occurring in the future and, as such, may put a Proactive MSP in place.

MSP Timeframes

When applying an MSP, Providers should consider a timeframe that is appropriate to the severity of the incident(s) and the Participant's behaviour. There are two timeframes that can be considered.

Provisional – 1 to 10 business days

- This timeframe may be applied as an immediate response following an incident and can provide a 'cooling off' period, if that is all that is required, or time to consider personal factors that may have contributed to the incident (see 'General Considerations') or any other circumstances on the day e.g.; physical environment, staffing etc.
- This will allow Providers time to decide whether to apply a Longer term MSP where necessary, and communicate with the Participant.

Longer term – 11 business days up to 12 months

- This timeframe provides a longer period for the Provider to address issues, provide support and manage interactions between the Provider and the Participant to ensure safety of all involved.

Servicing Arrangements and Restrictions under an MSP

Under an MSP, Providers can put in place the following restrictions or servicing arrangements:

- Partial or full service channel restrictions.
- One Main Contact (OMC) and back up OMC.
- Internal referrals, e.g. to in house counselling.
- External referrals to Services Australia for a re-assessment, or to other government or non-government services such as crisis accommodation.

The type of servicing arrangements/restrictions are at the discretion of the Provider and should be appropriate to the circumstances and proportionate to the behaviour or risk.

Note: All MSP arrangements must ensure that the Participant remains connected to employment services to meet their Mutual Obligations Requirements or compulsory participation requirements.

The Provider should ensure that the Participant understands the requirements of the MSP arrangements.

Channel Restrictions

The partial or full restriction of one or more service channels assists Providers in managing the impact of challenging behaviours by enabling them to limit a person's contact with them. Channel restrictions are:

Type	**Effect**
Face-to-face – full restriction	Participant cannot attend, in person, a site where the Provider delivers services.
Face-to-face – partial restriction	Participant has limitations on how, when and where they may access face-to-face services. For example, Participant is directed to attend the site at a particular time on a particular day.
Telephone - full restriction	Participant cannot contact the Provider by telephone.
Telephone – partial restriction	Participant has limitations on how and when they are able to telephone the Provider. For example, Participant is directed to call One Main Contact (OMC) only. (See '**One Main Contact (OMC)**').
Writing - full restriction	Participant cannot contact the Provider through any written or digital channel.
Writing - partial restriction	Participant has limitations on how they are able to write to the Provider. For example: Participant is directed to write to a single specific address; or Participant is directed to write to their OMC only

One Main Contact (OMC)

As part of the MSP, a Provider may decide to restrict a Participant to One Main Contact (OMC) within the organisation.

- The OMC should be named in the MSP and the specific details of how the Participant should contact or work with their OMC should be clearly outlined.
- A back up OMC should also be assigned and named in the MSP in the event the OMC is unavailable.

Internal Referral

As part of the MSP, Providers should consider whether the Participant would benefit from other **internal** services they might offer such as counselling. They should also check with the Participant to see if their

circumstances have changed and if appropriate, conduct a JSCI Change of Circumstances Reassessment (CoCR)

External Referral

As part of the MSP, Providers should consider whether the Participant would benefit from other **external** services. This could include referral for an ESAt to ensure the Participant has been appropriately streamed or referral to a range of services, including but not limited to, counselling services (if not available internally), housing assistance, crisis assistance, drug and alcohol rehabilitation or legal aid.

If Providers are unable to conduct a JSCI CoCr or a referral for an ESAt, they should discuss this with their Relationship Manager.

Approval to apply an MSP

All Provisional and Longer term MSPs require approval from a Site Manager or equivalent and must be recorded in the Departments IT System.

The Provider **must** advise the Department of Longer term MSPs **with** channel restrictions within 24 hours or as soon as possible by emailing their Relationship Manager.

Advising the Participant of MSP arrangements

Participants must be notified of the servicing arrangements and channel restriction/s in writing as soon as possible after the MSP arrangements have been finalised. This notification should also advise the Participant that they can request for the restriction/s to be reviewed at any time including at the time it was applied (see 'Participant's review/appeal').

Participants can be provided a letter:

- In person, if the Participant is on site,
- By postal delivery (Providers should consider registered post to ensure that they can confirm that the Participant has actually received the letter), or
- By email.

💻 **System step:** An example of a letter will populate as a guide only for Providers.

Review of MSPs including Participant's request for review/appeal

Participants can have their MSP reviewed at any time or appeal the MSP when it is applied or reviewed. Participants can contact the Department's National Customer Service Line (NCSL) to discuss the servicing arrangements in the MSP.

An MSP should be reviewed regularly (in particular, prior to it expiring) to assess any ongoing risk posed by the Participant. The review should also assess the suitability of transitioning the Participant back to standard service channels.

The Participant should be given the opportunity to participate in the review of the MSP. The Participant can request the review of their MSP at any time, including when it is initially applied (see 'Participant's review/appeal').

As part of the review, Providers should work through the MSP with the Participant where possible and safe to do so. If an agreement cannot be reached, the Provider should contact their Relationship Manager.

Note: If a 12 month MSP expires, it will not be automatically renewed and the Participant will no longer have any restrictions in place.

For a Longer term MSP, Providers should discuss options with the Relationship Manager to either extend the MSP (if there is a continued threat to safety), or transition the Participant off the MSP.

The outcomes of a review may be to:

- end an MSP and return a Participant to standard service channels
- apply a Longer term MSP following a Provisional MSP
- extend an MSP unchanged
- vary the MSP arrangements in place and set a new review date.

Additional reviews of an MSP can be initiated where Providers see fit, such as where a Participant's circumstances change, or there is a request for a review by either the Provider or Participant.

Breach of MSP arrangements

It is considered a breach when Participants do not follow the servicing arrangements and channel restrictions as set out in their MSP.

Where a Participant is in breach of the MSP, the Provider must lodge an incident report in the Department's IT systems.

Note: If the Provider identifies that the Participant was not aware of the MSP or channel restrictions (i.e. did not receive their letter) this should also be recorded.

Note: Where Participants repeatedly continue to breach their MSP and/or continue to be a threat to staff, Providers should escalate the matter to their Relationship Manager. Where necessary Relationship Managers will refer cases to the relevant team in the National Office of the Department for review and assistance in managing the behaviour.

Servicing Participants Post MSP and Channel Restrictions

Providers should consider and record in the Participant's MSP how the Participant will be serviced after transitioning back to standard servicing, once the MSP and channel restrictions have been lifted. Consideration should be given to what ongoing measures will be implemented to ensure, for example, improved behaviour by the Participant.

Transfers with an MSP or Serious Incident in Place

As some transfers are automatic (e.g. change of address), it is crucial that Providers record all details of an MSP to ensure the new Provider can access the information.

A decision should be made between the new Provider and the Relationship Manager about whether or not the MSP should be kept in place.

Where there is a Serious Severity or ES Level 3 incident report on a Participant's record in the Department's IT system, the Participant cannot be transferred to another Provider without the involvement of the Department. Providers should approach the Department through their Relationship Manager to authorise the request.

Note: As at June 2019, the Department's IT system has an additional transfer reason 'Transfer as a Result of a Serious Incident' where a transfer has occurred following a Serious incident.

Note: If a Participant transfers to a gaining Provider while an MSP is active, the new Provider must be made aware of existing requirements. This may include, where possible and appropriate, a phone call to the gaining Provider by either the current Provider or their Relationship Manager.

---

4. Summary of required Documentary Evidence

💻 **System step:** DES Providers must use the Incident Report screen in the Department's IT system to record all instances where a Participant exhibits challenging behaviours.

- **System step:** Any warnings given to a Participant must be recorded on the comments screen on the Participant's record in the Department's IT system.
- **System step:** Providers must record all MSP arrangements and restriction/s that are put in place in the MSP screen on the Participant's record in the Department's IT system.