

Withdrawn

This publication is withdrawn.

This publication is no longer current.

Provider Direct – Work Programme

Please Note: The Provider Direct service cannot be used for Universal Credit claim queries as the agents do not have access to the relevant IT systems or the required knowledge.

Contents

Introduction	1
Benefits of using the service	2
Raising a compliance doubt that attracts a Lower Level sanction (WP08).....	2
Raising a compliance doubt that attracts a Higher Level sanction (PRE01)	2
When to use the Provider Direct service	2
Circumstances when Provider Direct may not be appropriate	3
Change of Circumstances.....	3
Contacting Provider Direct	3
Multi Agency Public Protection Arrangement (MAPPA) and Special Customer Record (SCR) cases.....	3
Access code process	3
Access code security process.....	4
Process.....	4
Participant security check	5
Details to be checked.....	6
Recording evidence of the call	7
Agent ends call	8
Access codes.....	8
Action to take where a member of staff has left and a change in access code may be required.	9
Business Continuity	10
Annex A: Provider Direct – Desk Aide	11
Annex B: Potential Security Incident	13

Introduction

1. Provider Direct is a telephone helpline service for providers. It is for you to use when a Work Programme participant has failed to carry out a mandated activity and you are going to raise either:
 - a WP08 (Failure to take part in the Work Programme) form for a lower level sanction referral, or
 - a PRE01 (Refusal of Employment) form for a higher level sanction referral.
2. This service allows you to check that you hold the correct details prior to deciding whether or not to make a compliance doubt referral to DWP Labour Market Decision Making (LMDM) team.

3. The aim is to reduce the large number of inappropriate compliance doubt referrals, which will have clear benefits for both providers and DWP.

Benefits of using the service

4. The benefits of using this service include:
 - saving you resource and time by only having to complete a compliance doubt referral in appropriate circumstances
 - faster processing of compliance doubt referrals
 - the adverse decision rate should increase if inappropriate referrals are removed
 - reduction in the number of instances of potential negative participant behaviour towards you due to inappropriate referrals.
5. The Provider Direct service is not designed or resourced to act as a job outcome tracking service and must not be used for this purpose. If DWP finds that there are instances where this service is not being used for its intended purpose, we reserve the right to withdraw the service.
6. If this was to occur, you would need to provide assurance of compliance before access to the service could be re-instated.

Raising a compliance doubt that attracts a Lower Level sanction (WP08)

7. When you mandate a participant to an activity and they fail to carry out the activity, you must raise a compliance doubt referral on form WP08. If the claimant is a vulnerable ESA participant, please see [Work Programme Provider Guidance Chapter 4b – Safeguarding & Vulnerability](#).

Raising a compliance doubt that attracts a Higher Level sanction (PRE01)

8. When you mandate a participant to apply for or take up employment and it has been determined that they have refused or failed to do so, you must undertake the actions below before completing Refusal of Employment (RE) referral form (PRE01). Please see [Work Programme Provider Guidance Chapter 6 – Raising a Compliance Doubt](#).

When to use the Provider Direct service

9. You are strongly encouraged to use the service each time you are intending to raise a compliance doubt referral unless it is clear that to do so would be inappropriate.

Circumstances when Provider Direct may not be appropriate

- Has the participant already told you that they were unable to complete the mandated activity in advance of the appointment?
 - Have you received the Work Programme referral from Jobcentre Plus in the last two weeks?
10. If any of these situations apply it is very unlikely that there will have been a change in the participant's circumstances and consideration should be given to raising the compliance doubt referral as soon as possible.

Change of Circumstances

11. Currently a significant proportion of unnecessary compliance doubt referrals that are being made are caused by providers not having been aware about the participant's changes of circumstances.
12. The most common changes in circumstances that could lead to a participant failing to carry out a mandated activity include:
- participant has changed address and therefore not received notification of a mandated activity
 - participant is no longer in receipt of benefit.
13. While these are the two main reasons that a participant may not have carried out a mandatory activity, Provider Direct agents will inform you of any other change (that they are able to easily identify) that may lead to the participant's failure to take part.

Contacting Provider Direct

14. You are free to call as many times as you wish between the hours of 8am – 6pm, Monday to Friday, but you can only check the circumstances of up to 10 participants in any single call. If you need to enquire about more than this number, it will be necessary to call back. It is important that these restrictions are adhered to in order to allow agents to manage the volume of calls that they receive.

Multi Agency Public Protection Arrangement (MAPPA) and Special Customer Record (SCR) cases

15. If you have either a MAPPA or a SCR participant do not contact Provider Direct. You must contact your nominated Jobcentre Plus contact for information on these participants.

Access code process

16. Each provider will be allocated their own unique Provider Direct access code. The case-sensitive access code is sent out by our Business Management Team to the nominated Single Point of

Contact (SPoC) within the prime provider organisation on a monthly basis.

The role of the SPoC is to:

- take receipt of and manage the secure distribution of the access code
- ensure that all staff comply with the security plans relating to Provider Direct
- check to ensure that authorised users are using the correct access code following a change to it
- authorise changes of Provider Direct users should anyone leave the supply chain or change job roles
- take responsibility for resolving any complaints that may arise from Provider Direct agents
- notify DWP immediately should there be a change of circumstances that could affect the security of the Provider Direct access code, for example if a member of staff leaves who had access to the access code. Where this occurs a Potential Security Incident proforma ([Annex B](#)) must be completed and sent to WPD.SECURITY@DWP.GSI.GOV.UK
- any known or suspected breaches in security should be reported as per [Generic Provider Guidance Chapter 8 – Information Security](#).

Please see [paragraph 43](#) for more details.

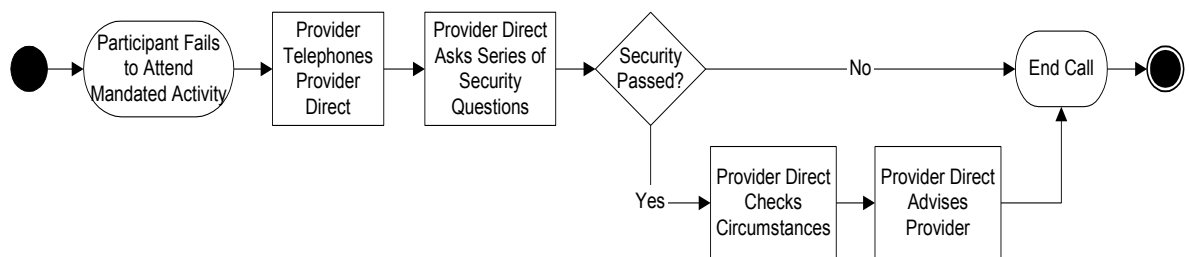
Access code security process

17. Before you can access the Provider Direct service you must provide DWP with the following:

- a detailed explanation of how you propose to keep the access code secure
- confirmation of whether or not your security plan will need updating – if so a Deed of Variation will be required.

18. If there are any changes to your access code security process you must inform DWP immediately.

Process



Confirm the caller is eligible to access the Provider Direct service

19. To use the Provider Direct service you will need to phone the dedicated Provider Direct telephone Number **0345 6044015**. Please note that to help maintain security, all calls will be recorded.
20. A Provider Direct desk aide is included at [Annex A](#) to help you provide and record any relevant information.
21. The Provider Direct agent will first confirm your eligibility to access the service by:
 - asking for the name of your company and your own name
 - the name of your prime provider
 - check your details against an approved provider list to confirm that you are eligible to use this service
 - determine the reason for your call.

Provider access code security check

22. The agent will conduct the access code security check. They will:
 - ask you to identify three random digits from an eight digit access code, for example, what is the second and fifth and eighth digit of the access code
 - check the access code against the monthly access code list which will be shared with providers as required.

If you correctly identify all three access code characters

23. The call will continue. Where you wish to discuss up to 10 participants during the call, it will not be necessary to ask further security questions.

If you fail to identify all three characters the agent will:

- inform you that you have failed the security questions
- advise you to call back when you have the correct access code
- end the call.

Participant security check

24. You will be asked for participant security details based on the information held on the original Provider Referral and Payment System (PRaP) referral from Jobcentre Plus to satisfy the security check.

Please Note: It is important that you have access to the original referral information listed below.

25. Please note that if you have updated this information on your internal systems then this will not match the information that

Provider Direct agents hold as they will only have information from the original referral.

26. Provider Direct agents do not have the capacity to deal with more than 10 participants in any one call. This will help to minimise the time you are waiting for your call to be answered.

Please Note: It is important to ensure that compliance doubt referrals are not stockpiled for too long.

27. The agent will ask you one security question which you must answer correctly for the call to continue.

28. The agent will ask you in respect of each participant:

The National Insurance number (NINO) and the full name of the participant and ask you **one** question from the following list:

- the claimant's Payment Group
- the referring officer's initials or name
- employment history (for example, last employer)
- selected qualifications
- the signing day and cycle
- the date of referral to the Work Programme.*

*Due to the way that the PRaP system updates overnight, the referral date that you receive is the day after the date that they were actually referred via the Jobcentre Plus Labour Market System (LMS). To accommodate this discrepancy, the Agent will accept the answer to the start date as being the **date held on LMS plus one day**.

For example, if the start date held on LMS is 6 November 2012 but you have 7 November 2012 on PRaP, this should still be accepted as a security pass.

29. The participant may not have any qualifications or work history and on occasions, information in LMS may be unclear. In this case Provider Direct agents will ask one of the remaining three questions.
30. If you fail the participant security check the agent will make a judgment on whether to:
 - move on to the next participant
 - advise you to call back when you have the correct details.

Details to be checked

31. Once you have passed the security questions, the agent will ask you the date the participant failed to carry out the mandated activity.

32. They will then ask you what details you wish to check, you can check the participant's:
- address
 - contact details – that is, phone number(s)
 - entitlement to benefit on the date they failed to take part – that is, whether or not in receipt of benefit.
33. They will also tell you about any other obvious changes in the participant's circumstances that are evident. They will not however be able to check for every change of circumstances or understand Work Programme policy or processes.
34. If the participant was in receipt of benefit on the day they failed to carry out the mandated activity and contact details are correct, the agent will advise you to raise a compliance doubt.
35. If the participant was in receipt of benefit on the day they failed to carry out the mandated activity and contact details held by the provider have changed (for example, change of address), the agent will advise you of the correct details and that you should not raise a compliance doubt.
36. If the participant was in receipt of benefit on the day they failed to carry out the mandated activity but the claim is now dormant, the agent will advise you to raise a compliance doubt. If the participant has gone into employment, where this information is held you will be advised of:
- the employer's name
 - start date
 - job title.
37. If the participant was not in receipt of benefit on the day they failed to carry out the mandated activity – the agent will advise you not to raise a compliance doubt. If the participant has gone in to employment, where this information is held you will be advised of:
- the employer
 - start date
 - job title.
38. If the participant is no longer in receipt of benefit but is not in employment, you will be advised of the reason if this is known.

Recording evidence of the call

39. Provider Direct will not be providing written evidence of any changes in circumstances that are identified.
40. It is therefore important that you record the advice given to you.
41. You should record:

- the date you called Provider Direct
- whether you were advised to raise a referral – if not, the reason for this.

Agent ends call

42. The agent will ask you if you have all the details you need and if you are clear what action you need to take. The call will then be ended.

Access codes

43. It is important to ensure that Provider Direct agents only answer calls from authorised and contracted Work Programme providers. To maintain security of participant's personal data, a rigorous system of security checks has been put in place to support this process.
44. A unique case-sensitive Provider Direct access code will be issued to each provider on a monthly basis and a private email will be sent to all of the named SPoCs DWP hold, containing an attached Microsoft Word document that is password protected.
45. On receipt of an acknowledgment from the SPoC, a separate email will then be sent to them containing the unlock code that is required to open the Word document.
46. It will then be the SPoC's responsibility to pass it on to the relevant people within their organisation in a secure manner.
47. The access code will be changed each month and the SPoCs will be emailed the new access code on the last Wednesday of the month, which will then to be used from the following Monday.

Access code changes and Security

48. It is important that security of participant's data remains our paramount priority, however we must balance this with the needs of the business in order to sustain an effective efficient service. We have therefore adopted a risk-based approach to keep any disruption to a minimum.

Instances when DWP would need to be informed of a change of circumstances that could require a change to the access code:

- if a member of staff leaves without giving notice, or they were subject to pending disciplinary procedures
- if a person has been dismissed
- if there is any reason to suspect fraudulent activity
- if a subcontractor organisation goes in to liquidation/ceases trading or terminates their subcontractor relationship with you

- any other scenario where there is the potential for a security breach.

This list is not exhaustive.

Instances when DWP would not need to be informed of a change of circumstances that could require a change to the access code:

- if a member of staff leaves to take up a new job and there is no reason to believe that they would do something inappropriate with the access code
- if a member of staff completes a temporary contract and there is no reason to believe that they would do something inappropriate with the access code.

Please Note: If you have any doubts at all about whether or not DWP should be informed, you should err on the side of caution and complete a Potential Security Incident proforma ([Annex B](#)).

Action to take where a member of staff has left and a change in access code may be required.

49. Where you believe that a change to the access code may be required you must complete a Potential Security Incident proforma ([Annex B](#)) and send it immediately to:

WPD.SECURITY@DWP.GSI.GOV.UK

Please Note: This email address is **only** to be used to send Potential Security Incident proformas. Any other Provider Direct issues/queries should be sent via your DWP Performance Manager.

50. Additionally, if you believe a security breach has occurred you must raise a security incident with DWP in the usual way.

WPD.SECURITY@DWP.GSI.GOV.UK

51. Upon receipt of [Annex B](#), DWP will assess all of the given circumstances and then decide if a change to the access code is required.
52. DWP will look at the reasons for the member of staff leaving to establish whether or not a change to the access code is required. Each case will be judged on its own merit.
53. If a change to the access code is required, the SPoC will be notified and a new code will be sent using the agreed change of access code procedures.

Complaint handling

Raising a Complaint about an individual Agent

54. If you need to raise a complaint about a specific agent you should ask to speak to their manager who will deal with your concerns. If you are still not satisfied with the manager's response you should then ask to speak to the line manager's own manager.

Raising a complaint about the Provider Direct Service

55. If you are unhappy with the service in general, for example the length of time you have been kept waiting or concerns about the security process, you should raise these issues with your DWP Performance Manager in the usual way providing any relevant evidence to support the complaint.

Business Continuity

56. In the unlikely event of a technical problem occurring leading to Provider Direct being unable to take calls, the SPoC will be contacted by a member of the DWP Business Management Team who will advise of the nature of the problem and how long the service is likely to be affected for.

Annex A: Provider Direct – Desk Aide

Before making the call

- Do I have the up to date Provider Direct Access Code?
- Do I know the name of my Prime Provider?

Remember: You will need to confirm three out of three access code characters correctly

- How many participants am I going to enquire about that have failed to carry out a mandated activity?

Remember: You can enquire about up to 10 participants in one call

From the original **PRaP referral information**, do I have details of:

- the participant's Payment Group
- the referring officer's initials or name
- the employment history (for example, last employer)
- the selected qualifications
- the signing day and cycle
- the date the each claimant was referred to the Work Programme.
- the date each participant failed to carry out the mandated activity?
- what information you need to know about each participant?
- whether each participant was still in receipt of benefit when they failed to carry out the mandated activity
- the correct address / phone number for each participant
- whether or not the participant started work? Is the employer/start date known
- anything else that is relevant?

To assist with Compliance Monitoring Officer checks, please update the participant's record with the date Provider Direct was contacted and the outcome of the discussion.

Recording the information

	Date signed off	New address	New phone number	Employment Details	Other	Date participant record updated
Participant 1						
Participant 2						
Participant 3						
Participant 4						
Participant 5						
Participant 6						
Participant 7						
Participant 8						
Participant 9						
Participant 10						

Annex B: Potential Security Incident

Please Note: Do not include personal details about any member of staff.

Prime Provider Organisation	Subcontractor Organisation	Date of Change of Circumstances	Reason for completion, for example, member of staff dismissed, subcontractor ceased trading. Please give as much information as possible

You must send the completed proforma to WPD.SECURITY@DWP.GSI.GOV.UK **immediately.**