Education & Skills
Funding Agency

Code of connection

Data Sharing Service for the National Careers Service

Version 0.2

This document helps users and organisations understand their obligations in integrating and sharing data with the National Careers Service

December 2017

Of interest to Prime Contractors and the National Careers Service National Contact Centre

Contents

Document management

Document control

Date	Version	Author	Description
01/11/2017	0.1	Wayne Busby	Creation of document and initial content
12/12/2017	0.2	Wayne Busby	Updates following first round of feedback

Document approval

Date	Version	Approvers

Interested parties

Party	Role

Document references

Title	Document location
CoCoR1 - Data dictionary	
CoCoR2 - Interface specification	
CoCoR3 - Service responsibilities	
CoCoR4 - Change process	

Purpose of document

This publication provides non-statutory guidance from the Education and Skills Funding Agency, it has been produced to help users and organisations understand their obligations in integrating and sharing data with the National Careers Service.

This document is completed by any organisation wishing to connect to the Data Sharing Service of the National Careers Service. It outlines the conditions that you need to meet and the information that you need to provide. This information will be used to assess whether you may connect/continue to connect to the Data Sharing Service. It may be necessary as part of the process to conduct an onsite assessment.

You must be in possession of a Data Sharing Service connection compliance certificate before you can connect to the service.

Who is this publication for?

This guidance is for:

- Prime Contractors of the National Careers Service;
- National Contact Centre;
- Technical staff, integration partners, security and data quality personnel, that need to design, manage and support the interfaces between their own systems and the National Careers Service.

Application process

1. To support your application, or re-submission for a compliance certificate, you must submit the following materials:

2. This Code of Connection document with all fields completed, including the signature of an authorised signatory of your organisation. The authorised signatory must be empowered to make legal commitments of behalf of your organisation;

3. An up to data network diagram, detailing your organisation name, date the diagram was created, local connections with approximate number of users, all external and third-party connections, location of security devices and geographical location of the network;

4. A recent (within the last three months) IT Health Check report and where applicable a remediation plan to address issues found;

5. A plan detailing connectivity and user testing cycles;

6. A recent (within the last three months) Cyber Essentials certificate.

Document structure

7. The document contains the following sections:

    7.1. Service responsibilities – The obligations of the organisation to react to actions of the customer and events within the wider service;

    7.2. Testing and technical responsibilities – The obligations on the organisation for implementing and testing their connectivity to the service;

    7.3. Data controls – The obligations of the organisation for the collection, quality, processing and sharing of information;

    7.4. Security – The obligations of the organisation to secure and protect the National Careers Service.

Service responsibilities

8. Your organisation is responsible for the collection, sharing, processing and consumption of information on behalf of the National Careers Service. This responsibility is based on an action or event being undertaken that directly affects the customer or the National Careers Service.

9. To facilitate a single service view of a customer and in support of an automated payment process your organisation is obliged to undertaken certain actions when certain events arise. This includes, but not limited to the following scenarios:

    9.1. Creation of a customer record;

9.2. Update to a customer record;

9.3. Merging of a customer record;

9.4. Deletion of a customer record;

9.5. Request digital account for migrated customer;

9.6. Customer transfers between touchpoints;

9.7. Creation of a careers and skills action plan;

9.8. Updates and acceptance of a careers and skills action plan;

9.9. Sharing adviser session availability;

9.10. Booking, updating and cancelling a careers advice session using adviser session availability;

9.11. Creation or update to an outcome;

9.12. Self-service activity;

9.13. Changes in reference data;

9.14. Changes in data schema.

10. Further details and rules of the obligations will be detailed in document CoCoR3 - Service responsibilities.

Testing and technical responsibilities

11. Your organisation is responsible for the testing, implementation, monitoring, support, maintenance and changing integration in line with the Data Sharing Service of the National Careers Service.
12. Your organisation will be expected to supply documentation and evidence in support of the following activities:
    12.1. Integration testing;
    12.2. Commitment to business acceptance testing;
    12.3. Involvement with end to end business testing;
    12.4. Business continuity testing;
    12.5. Active monitoring and alerting;
    12.6. Implementing a solution that caters for changes.

Data controls

13. To comply with the National Careers Service Code of Connection, the organisation must adhere and comply with the data control guidance laid out in this document. T
14. The guidance covers the following areas:

    14.1. Quality of data;

    14.2. Collection of data;

    14.3. Sharing and consumption of data;

    14.4. Duplication of data;

    14.5. Storage and processing of data;

Quality of data

15. Your organisation is responsible for the quality of data they manage on behalf of the National Careers Service. Data quality should be defined using clear quality control procedures that seek to actively manage and improve and assure the quality of data collected.

Collection of data

16. Customer and customer interaction data collected by your organisation on behalf of the National Careers Service should be proportional to its use. Your organisation should only collect data that is relevant to the user needs and is needed to perform your business function.

17. Where customer data is collected, your organisation is required to search existing National Careers Service customer records before creating a new one. All interactions between your organisation and that customer should then be recorded against that record.

18. Your organisation should adopt a ‘single service’ approach to dealing with customers and their data. All material interactions with a customer must be recorded against a customer record along with any resulting actions and responses. Where customers cannot be identified, statistical recording and categorisation of a customer query and response is required.

Sharing and consumption of data

19. Your organisation must share data at the earliest opportunity and no later than 24 hours where that data is relevant to the rest of the National Careers Service or the data is detailed in document CoCoR1 -Data dictionary.

20. Updates to your organisations records when originating from the Data Sharing Service must be trusted and applied at the earliest opportunity and no later than 24 hours. When updating data in your organisation at a date later than the interaction, it is your responsibility to ensure your records are up to date before committing changes and no subsequent data changes are overwritten. Where data updates are in doubt it is the responsibility of your organisation to raise the appropriate data challenge with the National Careers Service

21. Your organisation will consume reference data from the Data Sharing Service as detailed in document CoCoR1 -Data dictionary.

Duplication of data

22. It is the responsibility of your organisation to identify and merge duplicate records.

Storage and processing of data

23. All processing and storage of data must comply with security and information standards specified in this document and the terms and conditions of the National Careers Service.

24. Customer and service data should only be processes and accessed by staff/subcontractors for the purposes of delivery the Nation Careers Service.

Security

25. To comply with the National Careers Service Code of Connection, your organisation must have appropriate policies, processes and procedures in place to ensure the operational security of their infrastructure. This includes:

    25.1. Vulnerability management;

    25.2. Patch management;

    25.3. Secure configuration;

    25.4. Physical security;

    25.5. Protective monitoring and intrusion detection;

    25.6. End user devices and bring your own device (BYOD);

    25.7. Security incidence response;

    25.8. Authentication and access control;

    25.9. Boundary protection;

    25.10. Protection of data at rest;

    25.11. Protection of data in transit;

    25.12. User and administration separation;

    25.13. User management;

    25.14. Testing your security.

Vulnerability management

26. Your organisation must ensure you have a defined policy and supporting processes to identity, prioritise, resolve and mitigate vulnerabilities. Special consideration should be given for high and critical rated vulnerabilities.

Patch management

27. Your organisation must specify specific patching application and operating system periods along with a process for handling security and critical updates. Where updates cannot be applied mitigating actions must be specified and implemented.

Secure configuration

28. Your organisation must ensure that all IT systems, software and services are appropriately configured to reduce the level of inherent vulnerability. Any applications, services, processes and ports not required should be disabled by default and default passwords should be changed, especially administration access. All configuration changes should be managed through a controlled process where changes are recorded and appropriately approved.

29. All devices, systems and services should have the capability to detect, isolate and respond to malicious software.

Physical security

30. Your organisation will ensure that appropriately secure accommodation and appropriate policies and practices governing its use are in place to protect personnel, hardware, programs, networks and data from loss, damage or compromise.

Protective monitoring and intrusion detection

31. Your organisation must include processes and policies that include the detection and protection of potential and actual technical attacks as well as abuses or exploitation of business processes.

Security incidence response

32. Your organisation must be prepared for the occurrence of incidents, clearly demonstrating how the organisation will act to quickly contain the incident, limit harm, escalate where appropriate and learn from the incident.

33. For incidents that affect the wider National Careers Service appropriate reporting and escalation procedures must be defined. To aid investigation your organisation will, upon request provide audit logs, user activity logs, application exceptions and information security events to the National Careers Service.

Authentication and access control

34. Your organisation must ensure that user and application service accounts are provisioned with privileges appropriate to the need. The principle of least privilege

should be adopted where possible. Administration accounts must not be used to conduct day to day business, and should only be issued to users who need those privileges.

35. Your organisation must ensure and clearly demonstrate that all users authenticate themselves to use any devices, applications and systems and that the method of authentication is appropriate to the job they perform.

36. Any changes involving new starters, leavers and changes in role must also be catered for.

End user devices and bring your own device (BYOD)

37. Your organisation must provide policy that demonstrates any device accessing systems, applications and services are adequately protected, including the use of authentication, intrusion detection and prevention, virus protection, access management, data protection and retention of data. This should include the use of any mobiles, tablets and BYODs.

38. The National Cyber Security Centre (NCSC) have published guidance on end user device security and best practice information on BYOD Guidance - device security considerations.

Boundary protection

39. Your organisation will ensure that your network has appropriately configured boundary protection between their network and the internet or any other network. Network traffic, services and content should be limited or constrained to your business need via appropriate firewalls and access controls.

40. All network traffic should be encrypted and monitored to identify and remove malware. The organisation must ensure that any external connection to their network has an equivalent level of protection.

Protection of data at rest and in transit

41. Your organisation will ensure that all data will be protected by default whilst at rest and in transit. Protection covers both physical protection as well as data encryption protection. All OFFICIAL and above data must be encrypted at rest and in transit.

Users

42. Your organisation will ensure that users who have administrative privileges, access to OFFICIAL data or who are able to reconfigure networks undergo appropriate pre-employment checks which are aligned with the Baseline Personnel Security Standard

(BPSS). Organisation users must be trained to understand their obligations with regards to system security, data handling, and acceptable use.

Testing your security

43. Your organisation must implement regular IT Health Checks (ITHCs) and provide evidence that any security mechanisms put in place are ongoing and effective. The ITHC should identify any current vulnerabilities and any remediation work needed. Critical and High risks should be resolved immediately or else a viable plan for resolution must be agreed with the National Careers Service. Medium and Low risks may be accepted or subject to remedial action plans.

44. ITHCs will be conducted annually, but the National Careers Service may specify a different frequency of ITHCs where appropriate.

Security gaps

45. If you are not meeting any of the conditions above, please provide details below. Please also provide details where you are not meeting one of the conditions but are mitigating the associated risk with an alternate arrangement.

Commitment Statement

46. By signing this, you agree to the obligations spelled out in this document to be integrated with the National Careers Service. If you are unable or unwilling to meet any of these, you should inform the National Careers Service team immediately.

47. You agree to meet the Information Assurance (IA) and Security conditions outlined in the Code of Connection (CoCo), subject only to those exceptions specifically identified in your **Security Gaps** (above), and will submit the CoCo to the National Careers Service for a compliance assessment annually, or as required by the National Careers Service. If you have a concern that the conditions are not being met by other suppliers, you have a responsibility to notify the National Careers Service.

48. Upon receipt of a compliance warning notice, you must respond within five working days. You'll undertake suitable remedial action as directed by and agreed with the National Careers Service. If the National Careers Service rescinds your compliance certificate, you'll disconnect from the data sharing service in the timeframe specified.

49. Should the National Careers Service initiate a compliance review, you'll allow reasonable access to your site(s) and personnel within 25 working days of receiving notice of the review.

50. In the event of an incident, you must:

    50.1. Conduct initial diagnosis of the incident to determine which service is the cause (or most likely cause of the incident);

    50.2. Raise the incident with the National Careers Service;

    50.3. If the National Careers Service contacts you to help resolve an incident or problem, you must respond as you would for one of your own customers or users;

    50.4. Depending on the nature of the incident, provide audit logs holding user activities, exceptions and information security events to assist in investigations;

    50.5. Where your organisation uses subcontractors, you should manage incidents received from those suppliers on their behalf.

Authorised signatory

Name:	
Position:	
Telephone no:	
Email:	
Address:	
Date:	
Signed:	