

4.03 HRConnect Code of Practice

This policy is about

- The types of data held on HRConnect are detailed in [Section 3 Data held on HRConnect](#)
- Your rights to see data on the system is outlined in [Section 4 Access to Data held on HRConnect](#)

The following terms within this policy are defined in the glossary:

There are currently no terms within this policy defined in the glossary

You may also be interested in the following policies:

4.01 Personnel Records and Data Protection, 6.05 Equal Opportunities and Diversity

This policy is version 2.0

For a printable version please click the icon. Please make sure that your printed version is current with the one on this portal.

This homepage is only a guide to the policy, not the policy itself. In the event of any discrepancy between the content of this homepage and the associated policy, the wording of the policy shall apply.

4.03 HRCONNECT CODE OF PRACTICE

CONTENTS

- 1 Introduction3
- 2 Data Protection Act3
- 3 Data held on HRConnect3
- 4 Access to Data held within HRConnect4

4.03 HRCONNECT CODE OF PRACTICE

1 Introduction

1.1 This document reflects the changes in policy made necessary by the move from HRMS to HRConnect as part of the outsourced eHR services. It has replaced the Code of Practice C798/93 “HRMS Code of Practice”.

1.2 The services include both the computerised systems based on Oracle, in other words, Oracle HR, Oracle Payroll, Oracle CRM, Oracle Portal, and the telephony, email and white mail services provided by HRConnect.

1.3 This Code of Practice covers both the data held in HRConnect and the ways in which it is accessed and used.

1.4 A separate Code of Practice on Equal Opportunities monitoring exists covering access to data used for monitoring.

2 Data Protection Act

2.1 The HRConnect system fully complies with the requirements of the Data Protection Act 1998.

3 Data held on HRConnect

3.1 Data held on HRConnect covers personal information, resourcing, employee relations, learning and development, performance management, pay and reward and absence management. A full list of items held by the system is available on request.

3.2 Where it is necessary to fulfil the employment relationship between the employer and you, the staff member, HRConnect may share information with authorised data processors. An example of this would be sending information relating to you to a pension provider or HM Revenue and Customs.

3.3 The data in the HRConnect system is stored in an access-controlled, centralised and secure database located in Northern Ireland. The security of the HR and payroll information held on HRConnect is taken very seriously and included in the contract for the service. HRConnect is secured to the same level as the previous HR system, with all the usual technical measures in place. These include firewalls to protect against external network attacks, anti-virus software to protect against malicious software and access controls to ensure people can only see the information they need to see. HRConnect is housed in a local data centre backed up by two disaster recovery sites which are all physically secure. HRConnect staff are all cleared to the same security level as existing HR staff.

3.4 Access to HR data is restricted only to those who require it for the performance of their role and to the individual staff member to whom the data relates.

4 Access to Data held within HRConnect

Overview

4.1 The HRConnect system is based on the principle of permitting access to data to the most appropriate people at the most appropriate time. This constitutes secure, controlled access to data via a secure Intranet web browser and self-service screens for people performing authorised roles as set out in the following sections.

Subject access

4.2 The Data Protection Act 1998 provides the right of an individual to access personal information held about him or her by an organisation. The majority of employees will have direct system access to this personal information via HRConnect self service, and will be able to correct any factual errors and keep the information up to date as and when changes occur.

4.3 If you do not have access to self-service, you will, on a regular basis, be given transcripts of the main items of personal information held about you to provide an opportunity to correct any factual errors.

4.4 Under the Data Protection Act 1998, you also have the right to be provided with a copy of all of the information held about you by HRConnect. If you wish to exercise this right you should contact HRConnect.

Staff member access

4.5 In addition to the personal data access described in 4.2 above you have access to HRConnect in order to initiate transactions or track progress on cases associated with you personally.

4.6 Access to data is controlled by Northern Ireland Civil Service/Northern Ireland Office (NICS/NIO) secure network access, HRConnect User Identity and Password, and assigned HRConnect role.

4.7 In addition to personal information, you may also provide HRConnect with information about others such as emergency contact and next of kin. By entering and updating this information you are confirming that those persons are aware that their data has been provided to HRConnect and that they consent to NICS/NIO storing and using their data for the purposes for which it was provided.

4.8 By accessing HRConnect and viewing, updating or modifying data you are accepting responsibility for the impact of any incorrect amendments. You must not attempt to access data that you are not authorised to view. The following actions may result in disciplinary and/or criminal proceedings:

- Any attempt to access, modify or update another staff member's personal data;
- Any attempt to access, modify or update another staff member's job-related or pay-related data;
- Any attempt to access equal opportunities and/or community background data.

Note: If your role falls into any of the groups mentioned in sections below (4.9 to 4.13) then you will have additional access rights related to your operational role.

You may permit a clearly identified fellow employee to contact HRConnect on your behalf. If you wish to establish such a facility you must do so in advance using the appropriate form available on HRConnect. Please refer to [4.04 Contacting HRConnect User Guide](#) for process details.

Line manager access

4.9 In addition to the personal data access described in 4.1 and 4.2 above Line Managers have access to HRConnect in order to initiate transactions, authorise employee transactions, view job-related data and run some reports. Depending on the Line Manager's level of authority they will have the ability to initiate and/or authorise changes to data in accordance with NICS/NIO policies and procedures. Data access is limited to some information regarding those staff members within the Line Manager's span of control, in other words, the organisational hierarchy that they head. Line Managers will not, for example, be able to view their employee's personal information such as home address.

4.10 Access to data is controlled by NICS/NIO secure network access, HRConnect User Identity and Password, and assigned HRConnect role.

4.11 By accessing HRConnect and viewing, updating or modifying data the Line Manager is accepting responsibility for the impact of any incorrect amendments. Line Managers should not attempt to access data that they are not authorised to view. The following actions may result in disciplinary and/or criminal proceedings:

- Any attempt to access, modify or update a staff member's personal data;
- Any attempt to access, modify or update a staff member's job-related or pay-related data not in accordance with NICS/NIO policies and procedures;
- Any attempt to access equal opportunities and/or community background data

Departmental HR Access

4.12 Departmental HR has access to HRConnect in order to initiate transactions, authorise transactions, view employee data and run reports. Due to the nature of their work Departmental HR has wider access to HR & Payroll data for their Department. Departmental HR can also request scanned copies of correspondence and other relevant documentation from HRConnect.

4.13 Access to data is controlled by NICS/NIO secure network access, HRConnect User Identity and Password, and assigned HRConnect role. Departmental HR's access extends to include the HRConnect "professional screens" as opposed to "self service" but this access is on a limited, read-only, basis.

4.14 By accessing HRConnect and viewing, updating or modifying data the member of staff in Departmental HR is accepting responsibility for the impact of any incorrect amendments. Departmental HR should not attempt to access data that they are not authorised to view. The following actions may result in disciplinary and/or criminal proceedings:

- Any attempt to access, modify or update a staff member's data not in accordance with NICS/NIO policies and procedures;
- Any attempt to access equal opportunities and/or community background data identifiable to an individual staff member.

Welfare Officer Access

4.14.1 Within Departmental HR functions, Welfare Officers will have access to specific parts of HRConnect to enable them to record some basic details of cases. These parts of the system will only be accessible by Welfare Officers.

Health & Safety Officer Access

4.14.2 Within Departments, Health and Safety Officers will have access to specific parts of HRConnect to enable them to record details of incidents. Health and Safety Officers will only have access to those elements of the system which enable the recording of incidents.

Corporate access

4.15 Corporate HR have access to HRConnect in order to run reports on a service-wide basis. Due to the nature of their work Corporate HR have wider access to data for reporting purposes only. Individual employees will not be identifiable through the running of such reports. With the exception of those responsible for Equal Opportunities monitoring, Corporate HR will not have access to individual staff records.

4.16 Access to data is controlled by NICS/NIO secure network access, HRConnect User Identity and Password, and assigned HRConnect role.

Equal Opportunities Roles

4.17 Those formally responsible for Equal Opportunities monitoring or those required to undertake reporting and/or analysis of equal opportunities data will be granted access to run specific reports regarding equal opportunities data and trends. Equal Opportunities staff within Corporate HR will have access to monitoring data for all NICS staff for these purposes.

4.18 Equal Opportunities staff in the Northern Ireland Office shall have access to monitoring data for Home Civil Servants. This level of access will be restricted to the Northern Ireland Office and will not be available to NICS Corporate HR.

4.19 Access to data is controlled by security clearance, secure network access, HRConnect User Identity and Password, and assigned HRConnect role.

4.20 By accessing HRConnect staff performing an Equal Opportunities role accept responsibility for their actions. The following actions may result in disciplinary and/or criminal proceedings:

- Any attempt to access, modify or update a staff member's data not in accordance with NICS/NIO policies and procedures;
- Any attempt to acquire, share or use NICS/NIO staff member data for reasons outside of normal NICS/NIO operational procedures;

HRConnect Shared Service Centre Access

4.21 The HRConnect Shared Service Centre (SSC) has access to HRConnect in order to process transactions, update statuses, administer cases, view employee data in order to provide answers to queries and run reports.

4.22 Access to data is controlled by security clearance, secure network access, HRConnect User Identity and Password, and assigned HRConnect SSC roles. Access is via HRConnect "professional screens" and iRecruitment screens.

4.23 By accessing HRConnect and viewing, updating or modifying data the members of the HRConnect SSC accept responsibility for the impact of any incorrect amendments.

The following actions may result in disciplinary and/or criminal proceedings:

- Any attempt to access, modify or update data not in accordance with SSC procedures;
- Any attempt to acquire, share or use NICS/NIO staff member data for reasons outside of normal SSC operational procedures;
- Any attempt to access equal opportunities and/or community background data identifiable to an individual staff member unless specifically in order to perform an approved function, for example entering Equal Opportunities data from hard copy application forms.

HRConnect Service Management Access

4.24 The HRConnect Service Management Organisation (SMO) has access to HRConnect systems in order to maintain, support and enhance the service.

4.25 Access to data is controlled by security clearance, secure network access, HRConnect User Identity and Password, and assigned HRConnect role. The SMO role can be regarded as system administration for HRConnect services

4.26 By accessing HRConnect and investigating support requests the member of the SMO is accepting responsibility for the impact of any incorrect resolution. The following actions may result in disciplinary and/or criminal proceedings:

- Any attempt to access, modify or update data not in accordance with SMO policies and procedures;
- Any attempt to acquire, share or use NICS/NIO staff member data for reasons outside of normal SMO operational procedures;
- Any attempt to access equal opportunities and/or community background data identifiable to an individual staff member.

Access to Applicant Data

4.27 Any person applying for employment with NICS/NIO will have their full application details, including equal opportunities data, stored on the HRConnect system. Certain non-sensitive parts of this data, anonymised as appropriate, will be made available to Assessment Panels in order to sift, shortlist, assess and/or interview applicants. Such information will be provided in accordance with existing NICS/NIO policies.

4.28 Access to data is controlled by security clearance, secure network access, HRConnect User Identity and Password, and assigned HRConnect role. Only HRConnect and the Applicant will have direct access to the individual applicant record. Panel Members must accept responsibility for maintaining the confidentiality of the applicant information they handle. The following actions may result in disciplinary and/or criminal proceedings:

- Any attempt to access, modify or update an applicant's data not in accordance with NICS/NIO policies and procedures and UK Data Protection legislation;
- Any attempt to acquire, share or use applicant member data for reasons outside of normal NICS/NIO policies and procedures;
- Any attempt to access equal opportunities and/or community background data identifiable to an individual applicant.

4.29 Applicant data not held as part of any successful job offer or reserve pool will be purged after 5 years.

Worklist Access & Out Of Office Settings

4.30 Line Managers will receive notification of actions awaiting their attention through email and through their HRConnect worklist. Managers may grant access to their worklist to another manager possessing the same permission level. Managers granting access to their worklist through either the Worklist Access or Out Of Office functions should exercise care in doing so by granting access only where it is required to complete transactions. Managers should, as a matter of course, review any granting of access to ensure access is granted for no longer than necessary.