

Housing Delivery Division

Memorandum of Understanding between the Department for Work and Pensions and Local Authorities

2011 – 2012

Handling and protection of Department for Work and Pensions customer data

Version: 1.23

Date: 10 June 2011

Document Control

Key personnel

Title	Memorandum of Understanding between the Department for Work and Pensions and Local Authorities
Author	Malcolm Mattack
Approver	Sylvia Haslehurst
Status	FINAL

Version history

Version	Date	Summary of changes	Changes marked
1.00 – 1.11		Annual review	Yes
1.12	6 October 2010	MoU Workshop	Yes
1.13	5 November 2010	Changes from Workshop attendees	Yes
1.14 – 1.15	25 November 2010	Internal changes	Yes
1.16	13 December	Internal changes	Yes
1.17	14 March 2011	DTA addendum	Yes
1.18	24 March 2011	Internal changes	Yes
1.19	28 April 2011	Internal quality review	Yes
1.20	9 May 2011	BPSS amendment	Yes
1.21	11 May 2011	DWP Disciplinary change	Yes
1.22	18 May 2011	Internal quality review	Yes
1.23	10 June	Signed off	Yes

References

Document reference	Document title
Training Pack	CIS Learning Pack for Local Authorities
LA CIS Guide	Local Authority Customer Information System Guide
HMG Baseline Personnel Security Standard	HMG Baseline Personnel Security Standard
HMG Security Policy Framework	HMG Security Policy Framework
Guidance for local authorities on the use of social security data	Guidance for local authorities on the use of social security data

Contents

Document Control	1
Key personnel.....	1
Version history.....	1
References.....	1
Contents	2
Abbreviations	3
1. Purpose of the Memorandum of Understanding	4
Introduction.....	4
DWP and HMRC information.....	4
DWP requirements.....	4
HMRC requirements.....	5
Making use of DWP data.....	5
Employee Authentication Service.....	6
2. Definitions	6
Local authority.....	6
HM Government Protective Marking System.....	6
HB/CTB administration.....	6
Security incidents.....	7
3. Government approved secure communication channel	7
Contracted Service Providers – Government approved secure communication channel..	7
4. Legal requirements	8
Legal gateways and other legislation relating to the use of information obtained from DWP and HMRC.....	8
Criminal offences relating to the misuse of personal data.....	8
5. Terms and conditions of using DWP and HMRC data	9
Training.....	9
Document and data retention.....	9
Access control policy.....	10
Baseline Personnel Security Standard.....	10
Unspent criminal record checks.....	11
Remote working.....	11
6. Management checks	11
Monitoring access.....	11
7. Internal security	11
Action required for security incidents and disciplinary action.....	11
Withdrawing CIS access.....	12
Investigative support from HDD LASST.....	12
Signed Memorandum of Understanding	14
Agreement: Handling and protection of Department for Work and Pensions customer data and use of the the Data Transport Appliance.....	14
Appendix A	15
Confidentiality agreement.....	15
Declaration:.....	15
Appendix B	16
Home and remote workers.....	16
Appendix C	17
Disciplinary action – unauthorised CIS access.....	17

Abbreviations

BPSS	Baseline Personnel Security Standard
CIS	Customer Information System
CESG	Communications Electronic Security Group
CSP	Contracted Service Provider
CTB	Council Tax Benefit
DTA	Data Transport Appliance
DWP	Department for Work and Pensions
EAS	Employee Authentication Service
GPMS	HM Government Protective Marking System
HB	Housing Benefit
HDD	Housing Delivery Division
HDD LASST	Housing Delivery Division Local Authority Security and Support Team
HMRC	Her Majesty's Revenue and Customs
LA	Local Authority
LA CIS Guide	Local Authority Customer Information System Guide
LACI	Local Authority Claim Information
LAIID	Local Authority Input Document
MoU	Memorandum of Understanding

1. Purpose of the Memorandum of Understanding

Introduction

1.1 This Memorandum of Understanding (MoU) is between the Department for Work and Pensions (DWP) and your local authority (LA). It sets out the framework and operating policy through which the LA will access DWP and Her Majesty's Revenue and Customs (HMRC) customer data for the administration of Housing Benefit and Council Tax Benefit (HB/CTB).

1.2 The MoU has been approved by the Head of Housing Delivery Division (HDD) on behalf of DWP and by the Local Authority Associations. The MoU must be signed by the operational manager with responsibility for HB/CTB in the LA. It must be countersigned by the Section 151 Officer in England and Wales or in Scotland and Northern Ireland the officer accountable for the proper administration of financial affairs.

1.3 The counter signatory in the LA is responsible for ensuring compliance to safeguard the security of personal customer information.

DWP and HMRC information

1.4 DWP and HMRC personal data is information, which LAs may access and make use of in specific circumstances. Whilst this MoU primarily refers to information held on DWP's Customer Information System (CIS), which LAs access through desktop terminals it equally includes any data provided by DWP for the purposes of administering HB/CTB through whatever medium. As examples:

- electronically transmitted DWP information and hard copy
- information accessed and taken from CIS and stored, for example on local document imaging systems; and
- documents received from DWP via the Data Transport Appliance (DTA) server.

1.5 The DTAs are located in LAs and currently provides LAs with:

- Local Authority Claim Information documents (LACI's)
- Local Authority Input Documents (LAID's).

1.6 The DTA is the subject of an addendum to this MoU, which LAs must comply with.

1.7 DWP is constantly working to improve the way it exchanges data with LAs. The MoU will be reviewed at least annually to take account of these changes and any additional compliance requirements.

DWP requirements

1.8 DWP and LAs are committed to meeting statutory and mandatory obligations regarding the provision and accessing of personal data. The LA will ensure:

Housing Delivery Division – Memorandum of Understanding

- access to DWP data supplied to LAs will only take place from within the United Kingdom – no solution allowing individuals or contracted service providers (CSPs) access from abroad will be permitted
- all accesses to DWP data must be carried out using a government-approved IT channel and end point approved to access 'RESTRICTED' Impact Level 3 (IL3) information. More information can be found in the paragraphs relating to [HM Government Protective Marking System](#) (GPMS)
- proportionality – LAs will only access data necessary to carry out statutory functions in relation to the administration of HB/CTB
- accountability and consistency – by being accountable and able to justify decisions, maintaining strict policies and protocols made in relation to collection and onward sharing of data.

1.9 DWP's direction is that this MoU must be used to demonstrate assurance in respect of all data sharing between the 2 organisations. The data LAs access will improve HB/CTB administration and ensure those benefits are paid to the right people at the right time.

1.10 However, data sharing arrangements to improve customer service must ensure our customers' personal details are protected. By signing this MoU, the signatories for the LA acknowledge they understand and agree the:

- conditions for accessing DWP and HMRC data
- specific measures that must be in place to meet the terms of the agreement
- possible consequences of breaking the terms of this agreement.

HMRC requirements

1.11 DWP has an agreement with HMRC emphasising the commitment both central government departments have to ensure data security. DWP now works in partnership as a data processor with HMRC to provide LAs with direct access to tax credit data on CIS. HMRC provides this data to enable LAs to more effectively administer HB/CTB.

1.12 Any reference in the MoU to the security of customers' personal data incorporates any information supplied by HMRC; this includes tax credit and child benefit data. All current or proposed data transfers, or sharing of customers' personal data from HMRC, whether relating to individual customers or bulk transfers, must meet the security requirements of both DWP and HMRC. All data supplied is to be held within a secure environment, including all places where the data may flow, be stored or processed.

1.13 It should be noted HMRC will immediately suspend access to its data if any LA fails to meet security requirements or transfers or shares information without explicit approval from HMRC.

Making use of DWP data

1.14 DWP welcomes the opportunity to share data to provide better services and benefits to social security customers providing this is lawful and is done in

a secure manner. DWP provides LAs with data, which can be shared with other organisations (including other LAs) for the purposes of administering HB/CTB. This MoU must be read in conjunction with DWP's Local Authority CIS Guide (LA CIS Guide). More information can be found in DWP's [Guidance for local authorities on the use of social security data](#).

Employee Authentication Service

1.15 In 2010/11 DWP changed the way users in LAs access DWP and HMRC data systems. The Employee Authentication Service (EAS) project introduced strong registration processes to check and record the identity of end users and issued these users with an authentication device (token, used in conjunction with a PIN).

1.16 Users who have been through the registration process and issued with a token and PIN must use this method to access CIS and other relevant data systems when notified that their registration and enrolment has been authorised by the DWP National Registration Authority Hub. For further information on EAS contact nra.hub@dwp.gsi.gov.uk

2. Definitions

2.1 For purposes of this MoU, the following definitions apply.

Local authority

2.2 In addition to LAs who directly administer their HB/CTB service, the term 'authority' includes any CSP responsible for administering all or any part of the HB/CTB service on behalf of the LA from any permitted location.

HM Government Protective Marking System

2.3 HM Government Protective Marking System (GPMS) is designed to help individuals determine and indicate to others, the levels of protection required to prevent the compromise of valuable or sensitive assets. In this context asset includes DWP and HMRC data. GPMS is a means of signalling quickly and unambiguously, the value of an asset and hence the level of protection it needs.

2.4 The underlying principle is that the consequences of compromise are clearly indicated by the protective marking applied to documentary assets held on paper or electronically. The Cabinet Office has implemented a number of protective markings to be used throughout government. These are PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET.

2.5 The GPMS indicator LAs must apply when accessing or handling any DWP or HMRC customer information, is 'RESTRICTED' IL3.

Further information regarding the protective marking scheme can be found in [HMG Security Policy Framework](#).

HB/CTB administration

2.6 In this context HB/CTB administration includes any contact with customers relating to an award or potential claim, handling appeals, recovery

of overpayments, and investigation of suspected benefit fraud including DWP benefits. It also includes action concerning the disclosure of information as permitted by section 42 of the Welfare Reform Act 2007 and the secondary legislation made under it.

Security incidents

2.7 In the context of the MoU a security incident is defined as an accidental or deliberate attempt, whether successful or not, to make unauthorised access to or compromise DWP or HMRC data. The information may be held clerically or electronically. It takes into account breaches of confidentiality of information through the accidental, deliberate disclosure or loss of data to someone not authorised to receive it. It covers any case of unauthorised access or the suspected dishonest use of the data by any person acting for, or on behalf of the LA while carrying out duties in connection with their position.

3. Government approved secure communication channel

3.1 Access to DWP and HMRC data is dependent upon the LA using a government approved IT communications channel and end points suitable for the handling of information at RESTRICTED IL3. Further information can be sought from DWP Housing Delivery Division Local Authority Security and Support Team ([HDD LASST](#)).

3.2 The LA must at minimum meet the mandatory information assurance accreditation standard specified by DWP to ensure continued receipt of DWP and HMRC data.

3.3 The following constraints are applied in addition to controls mandated in the information assurance accreditation standard specified. DWP will not permit any solution which allows individuals or any CSP with responsibility for administering all or any part of the HB/CTB service on behalf of the LA from any location to access DWP data from:

- outside of the UK
- any location using WiFi or wireless 'dongles'.

3.4 These options are not permitted due to the vulnerabilities associated with using them.

Contracted Service Providers – Government approved secure communication channel

3.5 Where a CSP is engaged, continued access to DWP and HMRC data will also be dependent on both the LA and any CSP meeting at minimum, the government approved IT communications channel standard.

3.6 The LA must require CSPs to fully identify any part of HB/CTB service work it sub-contracts out to any other organisation.

3.7 Should the LA engage with or move to a different CSP, or changes occur to personnel who acted as signatories during the term of this MoU those changes must immediately be notified to [HDD LASST](#). This must be done on

an updated MoU form, which can be found on [page 14](#). Any new CSP engaged must meet the standards of and be fully compliant with the mandatory government approved IT communications channel standard specified by DWP.

4. Legal requirements

4.1 DWP and HMRC can legally share information with LAs for the purposes of administering HB/CTB. This data cannot be reused for another purpose unless the law allows it, as an example where the customer has given explicit consent and LAs have legal powers for the further use.

4.2 Parliament has attached special importance to the confidentiality of social security information and has made it a criminal offence for a person employed in social security administration to disclose information relating to a particular individual without lawful authority. This offence provision and other restrictions in social security legislation means LAs cannot consider sharing or reusing social security data in the same way they would share or reuse other data they hold.

4.3 DWP's [Guidance for local authorities on the use of social security data](#) provides more detailed advice and staff involved in handling and processing social security data should ensure they are familiar with the information it contains.

Legal gateways and other legislation relating to the use of information obtained from DWP and HMRC

4.4 This MoU is underpinned by legislation which binds DWP and the LA to handle customers' personal information in confidence. This includes the:

- Data Protection Act 1998
- Social Security Administration Act 1992
- Computer Misuse Act 1990
- Tax Credit Act 2002.

Criminal offences relating to the misuse of personal data

4.5 There are a number of offences under the Data Protection Act 1998, Social Security Administration Act 1992 and Computer Misuse Act 1990 relating to unauthorised access to and use of personal data.

4.6 Section 55 of the Data Protection Act 1998 makes it an offence to:

- obtain, disclose or procure the disclosure of personal information, without the authority of the data controller, except in circumstances specifically allowed by law, such as the prevention of crime
- sell, or to offer to sell personal information obtained illegally.

4.7 Section 123 of the Social Security Administration Act 1992 makes it an offence for anyone who is or has been employed in social security administration to disclose personal information acquired in the course of their employment without lawful authority.

4.8 Section 115 of the Act allows criminal proceedings to be taken against corporate bodies (such as a LA) and officers where:

- an offence has been committed under the Act and
- it occurred with the consent or connivance of officers of the LA, or because of their neglect.

4.9 Section 1(1) of the Computer Misuse Act 1990 makes it a criminal offence for any person to cause a computer to perform a function with intent to secure access to any program or data held in any computer where the person:

- intends to secure an unauthorised access and
- knows at the time when they cause the computer to perform the function that is the case.

4.10 It is essential the LA recognises that in serious cases, where unauthorised access has been made, proceedings may be taken against the LA or its officers if it can be shown that negligence contributed to the disclosure.

5. Terms and conditions of using DWP and HMRC data

Training

5.1 DWP requires the LA to ensure that before prospective users are granted access to 'RESTRICTED' IL3 information they successfully complete appropriate data protection training. It is also a CIS specific requirement that any person successfully completes the technical and security training pack. Copies of the training packs are available from [HDD LASST](#).

5.2 When the training has been completed and before access is granted each prospective user must fully complete and sign the Confidentiality agreement ([Appendix A](#)).

5.3 The LA will be required to retain:

- a list of those who have received technical and security training, including the date they completed this training
- fully completed and signed Confidentiality agreements.

5.4 Until the LA has EAS two-factor authentication there will be a need to continue recording and securely retaining records of all CIS users registered on the Government Gateway and their unique 12 alpha-numeric digit identity.

Document and data retention

5.5 The Data Protection Act 1998 contains principles which organisations must follow when handling personal data. The principles do not specify retention periods for documents or data. It is for the LA to apply Principle 4 of the Data Protection Act 1998 to DWP and HMRC personal data it holds and the service it provides.

5.6 In general terms all DWP and HMRC data must be securely deleted from all systems or destroyed as soon as it is no longer needed for operational purposes.

Access control policy

5.7 An access control policy must be maintained for all DWP and HMRC information held. The policy will ensure that appropriate security mechanisms are in place and specify:

- access rights for individual users, or groups of users to DWP and HMRC information, based on the GPMS of the information and the 'Need to Know' principle
- the frequency with which reviews of access rights must take place for users
- action to be taken to remove access when there is no longer a business need. This includes changing jobs or roles
- the period after which inactive accounts must be suspended.

5.8 The policy will instigate a process ensuring all users and contractors who terminate their employment or relationship with the LA are aware of their obligation not to divulge information gained during their employment.

5.9 The policy must take into account where a segregation of duties needs to be applied. There are duties, which must not be done or managed by the same employees. As an example, it must not be possible for the same individual to verify their own actions where those actions are sensitive enough to require verification.

Baseline Personnel Security Standard

5.10 To access government assets, which includes personal customer information, LAs must comply with [HMG Baseline Personnel Security Standard](#) (BPSS). Any person who regularly uses DWP 'RESTRICTED' IL3 information, must be at least cleared to BPSS.

5.11 DWP does not require the verification checks for BPSS to be applied retrospectively for existing staff where pre-employment screening controls have already been carried out. However, any existing employee who is newly assigned and any employee recruited in the future to a post where access to government assets is necessary will need to be subject to BPSS verification checks.

5.12 Agency and CSP staff must be subject to the same pre and post appointment checks as permanent staff. LAs must not assume employment agencies or CSPs have carried out the prerequisite BPSS checks on staff supplied or recent periods of employment with DWP or other LAs guarantees the integrity of an individual. The LA is responsible for confirming any CSPs providing all or part of the HB/CTB service have carried out BPSS screening. The LA must have procedures in place for confirming these checks have been completed.

Unspent criminal record checks

5.13 Full implementation of BPSS, now includes a 100% application of the unspent criminal record check, (Basic Disclosure). This is now explicitly mandated as part of [HMG Security Policy Framework](#). The BPSS check for unspent criminal records does not have to retrospectively applied where pre-employment controls have been completed for existing staff. The check does apply to existing employees who are newly assigned and any employee recruited in the future to a post where access to government assets is necessary.

Remote working

5.14 All of the rules above apply equally to staff accessing DWP and HMRC data from outside of the office environment. Home and remote working is permitted but the LA has to recognise they represent an additional risk. Any remote working solution must be supported by a formal remote working policy. Additional mandatory requirements are detailed at [Appendix B](#).

6. Management checks

Monitoring access

6.1 To provide assurance access to DWP and HMRC data is appropriate and that information obtained has been used correctly, the LA must carry out the predetermined level of Management Checks (sometimes referred to as test checks). Further details are in the LA CIS Guide.

6.2 Please note HDD LASST and HMRC conduct additional risk-based checks as appropriate to confirm accesses to CIS have been performed in line with guidance.

6.3 The Section 151 Officer for LAs in England and Wales or in Scotland or Northern Ireland the Officer accountable for the proper administration of financial affairs will ensure clear and auditable processes are in place to independently carry out Management Checks.

7. Internal security

Action required for security incidents and disciplinary action

7.1 Suspected misuse of DWP and HMRC data or security incidents must immediately be reported to [HDD LASST](#) and a thorough internal investigation conducted. The LA will ensure there are processes in place to immediately notify HDD LASST of any:

- actual or suspected security incidents involving any data sourced from DWP or HMRC
- identified information or system faults.

7.2 The LA will ensure its formal disciplinary process and any relevant outsourcing arrangements provide for the investigation of individuals who

have allegedly committed or attempted a breach of the security framework set out in this MoU.

7.3 In circumstances where a person deliberately accesses, attempts to access or browses DWP and HMRC data without a legitimate business reason or appropriate authorisation the breach of security is considered to be extremely serious. The starting point for any security breach in DWP where a case to answer is found; is treated as 'Serious Misconduct'. This is the case even if it is established the information has not been misused.

7.4 Where an investigation is being carried out the LA will be required to provide [HDD LASST](#) with regular progress updates. When the investigation is completed DWP will require details of the final outcome.

7.5 A decision maker in the LA or any CSP administering all or part of the service on behalf of the LA from any location will comply with existing disciplinary processes and decide whether:

- misconduct has occurred
- disciplinary action is required
- the misconduct offence is:
 - Serious or
 - Gross, and;
- what disciplinary penalty to impose.

7.6 It is not possible to give an exhaustive list of the reasons why an employee might face disciplinary action. [Appendix C](#) illustrates some scenarios and the level of misconduct that would be applied in DWP where it is established there is a case to answer. It outlines what penalties may be applied for the different levels of misconduct according to the seriousness of the offence.

Withdrawing CIS access

7.7 In circumstances where it has been alleged an individual has made unauthorised access to DWP and HMRC data, and there is a case to answer DWP will in addition retain the right to impose a period of suspension from CIS.

7.8 DWP and HMRC maintain absolute discretion to withdraw access to the data supplied on CIS or any other data stream including LAIDs, LACIs and the HBMS scans. This situation may apply if it is considered if an LA as a whole is not complying with the conditions set out in this MoU. Access to data may also need to be withdrawn for operational reasons.

Investigative support from HDD LASST

7.9 DWP will support the LA to ensure appropriate disciplinary or prosecution action is taken in all cases. On more serious cases, DWP will consider taking its own prosecution action against individuals.

Housing Delivery Division – Memorandum of Understanding

7.10 [HDD LASST](#) will support the LA in conducting investigations and will, on request, arrange for the provision of system audit trails, which show the full CIS access history of any user.

Signed Memorandum of Understanding

Agreement: Handling and protection of Department for Work and Pensions customer data and use of the Data Transport Appliance

This agreement for controlling access to DWP and HMRC data has been approved by the Head of Housing Delivery Division on behalf of DWP and by the Local Authority Associations. It will remain in place until **1 July 2012**. It is signed on the understanding the signatories accepts the authority will comply with all aspects of the MoU. This includes use of the Data Transport Appliance.

It must additionally be countersigned by the authority's Section 151 Officer in England and Wales (or the officer accountable for the proper administration of financial affairs in authorities in Scotland or Northern Ireland) and by any appropriate Contracted Service Provider.

I have responsibility for staff access to DWP and HMRC data. I am satisfied the LA complies with the terms of the agreement and understand that non-compliance, depending on the seriousness of any incident, could result in the service being withdrawn and prosecution of individuals. It may result in access being withdrawn from the LA if it does not comply with the conditions set out in this MoU.	
Signed:	
Name:	
Full contact details:	
Position in the: <ul style="list-style-type: none"> LA; or Contracted Service Provider. 	
Full name, address and contact details of the: <ul style="list-style-type: none"> LA; or Contracted Service Provider. 	
GCSX, GSE or GSX email address:	
Date:	

Section 151 Officer (England and Wales) or the officer accountable for the proper administration of financial affairs in authorities in Scotland or Northern Ireland.	
Counter signed:	
Name:	
Full contact details:	
GCSX, GSE or GSX email address:	
Date:	

Appendix A

Confidentiality agreement

This form is to be signed by all staff prior to accessing DWP and HMRC data.

Declaration:

I have successfully completed full technical and security training. My attention has been drawn to the provisions of section 123 of the Social Security Administration Act 1992 and the Data Protection Act 1998. I understand:

- I may face prosecution and dismissal for any offence in respect of any unauthorised or attempted access to CIS or misuse of any DWP or HMRC data
- it is a criminal offence for me to access and or process DWP or HMRC data for any purpose other than HB/CTB administration
- I must not communicate official information or knowledge acquired in the course of my official duties whether written or oral, to anyone who is not authorised to receive such information
- upon termination of my contract of employment, I will continue to be bound by these provisions
- I must not:
 - use CIS to access or attempt to access my own record, the records of friends, relatives, partners, or acquaintances or make enquiries for colleagues in respect of their friends, relatives, partners, or acquaintances
 - share or allow any other person to use my system, Government Gateway, Employee Authentication Service token or other identity password
 - use CIS for any unauthorised purpose
- if there is any reason to believe I have breached this agreement, appropriate legal action may be taken against me.

Date training completed:	
Signed:	
Name:	
Date of declaration:	
Local authority:	

Appendix B

Home and remote workers

Office based IT systems generally have more robust security than IT applications used in the home or remotely, which pose greater risks that can be exploited. DWP understands the benefit of employing home and remote workers but needs to ensure the additional security risks are minimised. The LA will set down clear policies for remote working and ensure additional security training is given to staff that handle 'RESTRICTED' IL3 information and work outside of an office environment.

Please note: any person working away from the office environment will be required to operate EAS two-factor authentication.

Access to DWP and HMRC data is dependent on the LA having a government approved secure IT channel and the mandatory information assurance accreditation standard specified by DWP.

Any mobile, remote and or home working solution must at minimum comply with HMG Information Assurance Policy and Guidance.

In respect of this MoU this is Communications Electronic Security Group (CESG) Good Practice Guide No.10).

In addition to the contents of the MoU, prior to granting access to any DWP or HMRC data to workers from outside an office environment, your LA will:

- provide a list of home and remote workers' names to [HDD LASST](#)
- ensure measures are taken to prevent copying of DWP data to portable media, as examples
 - laptop computers
 - CDs
 - external hard drives and
 - USB memory sticks
- ensure screen prints are not left where any unauthorised person can see them. Any screen prints taken are to be shredded or disposed of through a managed confidential waste disposal service.

Appendix C

Disciplinary action – unauthorised CIS access.

The following tables are comparable to DWP’s disciplinary policy. If the LA finds there is a case to answer in respect of unauthorised access to CIS it should be used as a guide when deciding on the level of misconduct and any disciplinary action taken. HDD LASST will also provide further help on individual cases as required.

In all cases it is understood the decision on whether there is a case to answer will be made in discussion with a Human Resources manager in the LA. While the final decision regarding disciplinary action is in the control of the LA, DWP has absolute discretion to withdraw access to CIS where any individual user is suspected of misusing the system or where it considers the LA is not complying with the conditions set out in this MoU.

CIS users have an obligation to handle all data in accordance with the MoU. Access to any customer record held on CIS must be for a legitimate business reason. CIS users working for the authority must NOT access:

- their own account
- the accounts of friends or acquaintances or anyone directly related to them without a legitimate business reason
- personal customer data without authorisation.

Scenario 1.	Level of misconduct	Disciplinary Outcome
Browsing customer data	SERIOUS MISCONDUCT	Possible outcome – final written warning
A CIS user accesses or browses through customer data and records without legitimate business reasons or appropriate authorisation. They only access one	Where there is a case to answer the level of misconduct should be no less than serious misconduct.	This breach is extremely serious. Isolated incidents are likely to result in a minimum of a final written warning.

Housing Delivery Division – Memorandum of Understanding

record and there is no evidence of misuse.	Mitigation should only be accepted in very exceptional circumstances.	
In these or similar circumstances DWP will impose a 6 – 12 month exclusion from accessing CIS.		

Scenario 2.	Level of misconduct	Disciplinary Outcome
<p>Browsing customer data on more than one occasion.</p> <p>A CIS user accesses or browses through multiple customer records without a legitimate business reason or appropriate authorisation.</p> <p>This is referred to as multiple accesses (which may happen on the same day or over a period of time). There is no evidence that the information has been misused.</p>	<p>GROSS MISCONDUCT</p> <p>Where there is a case to answer the level of misconduct should be no less than gross misconduct.</p> <p>Mitigation should only be accepted in very exceptional circumstances.</p>	<p>Possible outcome – dismissal</p> <p>This breach is extremely serious.</p> <p>More than one breach is likely to lead to dismissal.</p>
In these or similar circumstances DWP will generally impose a 12 – 24 month exclusion from accessing CIS.		

Scenario 3.	Level of misconduct	Disciplinary Outcome
<p>Browsing your own record or those of their family, friends or celebrities</p>	<p>Gross misconduct</p>	<p>Possible outcome - dismissal</p>

Housing Delivery Division – Memorandum of Understanding

<p>A CIS user accesses their own personal record or those of their family, friends or celebrities without a legitimate business reason or appropriate authorisation. They access more than one record which makes this offence more serious.</p>	<p>Where there is a case to answer the level of misconduct should be no less than serious misconduct. Mitigation should only be accepted in very exceptional circumstances.</p>	<p>This breach is extremely serious. Isolated incidents will result in a minimum of a final written warning.</p>
<p>In these or similar circumstances DWP will generally impose a 12 – 24 month exclusion from accessing CIS.</p>		

Scenario 4.	Level of misconduct	Disciplinary Outcome
<p>Accessing records to falsify benefit claims</p> <p>A CIS user has authorisation to access personal sensitive data or information as part of their normal duties. They access records without legitimate business reasons and appropriate authorisation and use this information themselves (or on behalf of a third party) for personal gain, or to falsify claims for benefits.</p>	<p>GROSS MISCONDUCT</p> <p>Where there is a case to answer the level of misconduct should be no less than gross misconduct. Mitigation should only be accepted in very exceptional circumstances.</p>	<p>Possible outcome – dismissal</p> <p>Fraud is a serious criminal offence. All allegations will be fully investigated and where appropriate offenders prosecuted. This breach is extremely serious and is likely to lead to dismissal.</p>
<p>In these or similar circumstances DWP will generally impose a permanent exclusion from accessing CIS.</p>		

Scenario 5.	Level of misconduct	Disciplinary Outcome
-------------	---------------------	----------------------

Housing Delivery Division – Memorandum of Understanding

<p>Browsing information for personal gain</p> <p>A user deliberately accesses or browses through CIS records of without authorisation or legitimate business reasons and obtains sensitive information about an individual’s financial position. The employee uses this information for their own personal gain.</p>	<p>GROSS MISCONDUCT</p> <p>Where there is a case to answer the level of misconduct should be no less than gross misconduct.</p> <p>Mitigation will only be accepted in very exceptional circumstances</p>	<p>Possible outcome – dismissal</p> <p>This breach is extremely serious and is likely to lead to dismissal.</p>
<p>In these or similar circumstances DWP will generally impose a permanent exclusion from accessing CIS.</p>		